

Mobile First Base Designs Lab for ArubaOS 8

Authors:
Ben Lowe
Andrew Tanguay

Validated Reference Design

Copyright Information

Copyright © 2018 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA



www.arubanetworks.com

3333 Scott Blvd

Santa Clara, CA 95054

Phone: 1-800-WIFI-LAN (+800-943-4526)

Fax 408.227.4550

Revision History	6
About This Guide	7
Overview	7
Intended Audience and Assumptions	7
Scope	7
Reference Material	8
Related Documents	9
Conventions	9
Topology	14
Recommended Architecture	14
Test Lab Network Topology	16
Hierarchical Configuration	17
ArubaOS 8 Controller Modes	17
ArubaOS 8 Enhancements	20
Configuration Best Practices	27
Tunneling and Control Plane Security	31
Tunnel Mode	31
Decrypt-Tunnel Mode	32
Control Plane Security	33
Boot Process with Control Plane Security	34
Clustering	35
Benefits and Considerations	36
Local Management Switch	37
Cluster Roles	39
Change of Authorization	43
Network Management	50
Topology Description	50

Monitor Only Mode	51
Groups and Folders.....	52
Device Discovery	52
Network Access Control	53
Lab Design and Addressing.....	54
Service Set Identifiers.....	54
Guest Access.....	56
802.1X Authentication.....	60
BYOD SSID Configuration.....	61
Lab Setup.....	64
Configuration	67
SW-TOR-LAB	68
SW-Core	71
SW-Access-01.....	76
MM-01 Initial Setup	77
MM-02 Initial Setup	78
MM-01 Redundancy	79
MM-02 Redundancy	80
MM-01 Licenses.....	81
MC-01 Initial Setup	83
MC-02 Initial Setup	85
MC-03 Initial Setup	87
MC-04 Initial Setup	89
MM-01 Remaining Configuration	91
Employee BYOD SSID Configuration	98
HTTPS Server Certificate for MCs	102
BYOD Employee ClearPass Configuration.....	104
BYOD Employee Onboard Configuration.....	124
PSK SSID Configuration	132
AP Configuration	133

Firewall-DMZ.....	134
SW-AGG-DMZ.....	137
DMZ Configuration.....	138
Guest ClearPass Configuration.....	151
Guest Authentication with MAC Caching Wizard.....	156

Revision History

The following table lists the revisions of this document:

Revision	Date	Change Description
1.0.0	8/3/2018	Initial Publication
1.0.1	8/15/2018	Minor edits from initial feedback

Table 1 *Revision History*

About This Guide

Overview

Aruba Validated Reference Design Guides (VRDs) are best practice recommendation documents specifically designed to demonstrate the key functions of the Aruba solution and enable customers who deploy Aruba solutions to achieve optimal results. This document is not only intended to serve as a deployment guide but also to provide descriptions of Aruba technology, recommendations for product selections, network design decisions, configuration procedures, and best practices. The Aruba documentation suite for ArubaOS 8 comprises a reference model for understanding Aruba technology and offers designs for common customer deployment scenarios. Aruba customers rely on these proven designs to rapidly deploy Aruba solutions in their production environments with the assurance that they will reliably perform and scale as expected.

Intended Audience and Assumptions

The Mobile First Base Designs Lab VRD is intended for administrators who already possess a working knowledge of ArubaOS 8 concepts and who have already read the Fundamentals Guide. Aruba strongly recommends that readers review the [ArubaOS 8 Fundamentals Guide](#) on the Aruba Community site prior to reading first. This document was published as a follow up to the Fundamentals guide and both documents were intended to be read in tandem with each other.

Scope

The Validated Reference Design series documents focus on particular aspects of Aruba technologies and deployment models. Together these guides provide a structured framework to understand and deploy Aruba Wireless Local Area Networks (WLANs). The VRD series has four document categories:

- **Foundation** guides explain the core technologies of an Aruba WLAN. These guides also describe different aspects of planning, operation, and troubleshooting deployments
- **Base Design** guides describe the most common deployment models, recommendations, and configurations
- **Application** guides build on the base designs. These guides deliver specific information that is relevant to deploying particular applications such as voice, video, or outdoor campus extension.
- **Specialty Deployment** guides involve deployments in conditions that differ significantly from the common base design deployment models, such as high-density WLAN deployments.

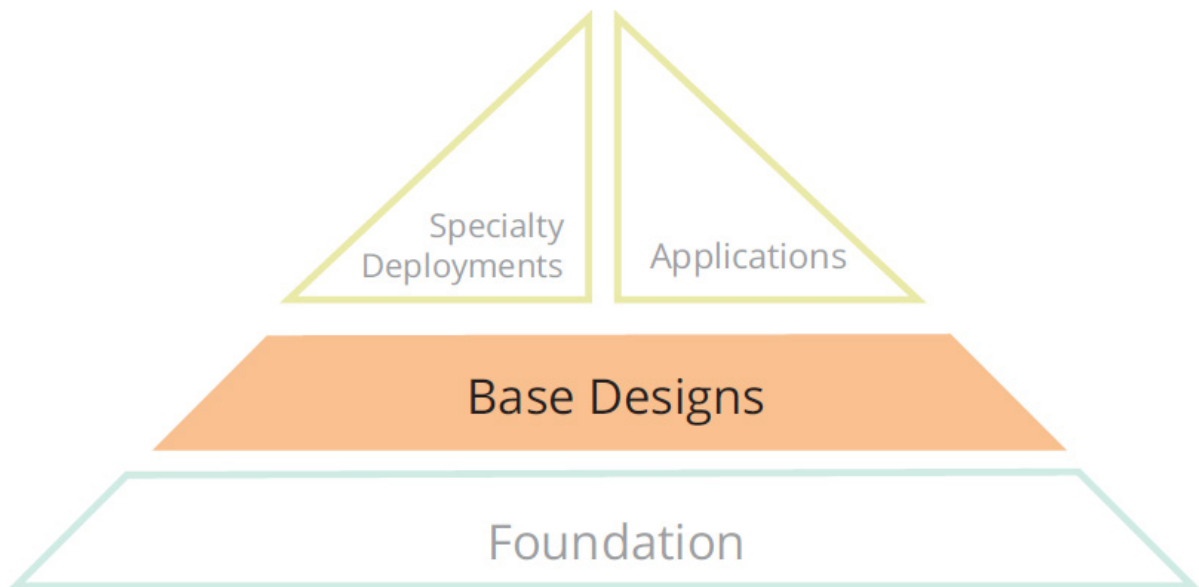


Figure 1 Aruba Reference Architectures

The Mobile First Base Designs Lab VRD is considered a Base Design guides within the VRD core technology series. The design described in this document is intended for single stack IPv4 users with small to medium size campus deployments. For additional details on designs for different sized deployments please refer to the Reference Architecture chapter of the [ArubaOS 8 Fundamentals Guide](#).

Reference Material

Readers should have a solid working understanding of basic wireless LAN concepts as well as the Aruba technology explained in the foundation level guides in order to read this VRD. The following resources will assist readers who require the knowledge necessary to digest this document in the intended manner:

- For information on Aruba Mobility Controllers and deployment models, please refer to the [Aruba Mobility Controllers and Deployment Models Validated Reference Design](#)
- The complete suite of Aruba technical documentation is available for download from the [Aruba Support Site](#). These documents present complete, detailed feature and functionality explanations beyond the scope of the VRD series.
- For more training on Aruba products or to learn about Aruba certifications, please visit the Aruba [Training and Certification page](#). This page contains links to class descriptions, calendars, and test descriptions.
- Aruba hosts a user forum site and user meetings called [Airheads Community](#). The forum contains discussions of deployment best practices, products, and troubleshooting tips. Airheads is an invaluable resource that allows network administrators to interact with each other and Aruba experts.

Related Documents

The following documents may be helpful as supplemental reference material to this guide:

- [ArubaOS 8 Fundamentals Guide](#)
- [ArubaOS 8 User Guide](#)
- [ArubaOS 8 CLI Reference Guide](#)
- [Aruba Solution Exchange](#)
- [ClearPass User Guide](#)
- [ArubaOS Switch User Guide](#)

Conventions

Typographical Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Style Type	Description
<i>Italics</i>	Italics are used to emphasize important terms and to mark the titles of books.
Bolded > words	Bolded words indicate an option that should be selected in the Graphical User Interface (GUI). The angled brackets indicate that the choices are part of a path in the GUI.
Command Text	Command text in this font will appear inside of a box and indicates commands that can be entered into the Command Line Interface (CLI).
<Arguments>	<p>In the command examples, italicized text within single angle brackets represents items that should be replaced with information appropriate to your specific situation. For example:</p> <pre># send <text message></pre> <p>In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.</p>
[Optional]	Command examples enclosed in brackets are optional. Do not type the brackets.
{Item A Item B}	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Table 2 *Typographical Conventions*

Informational Icons

The following informational icons are used throughout this guide:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to your hardware or loss of data.



Indicates a risk of personal injury or death.

Graphical Icons

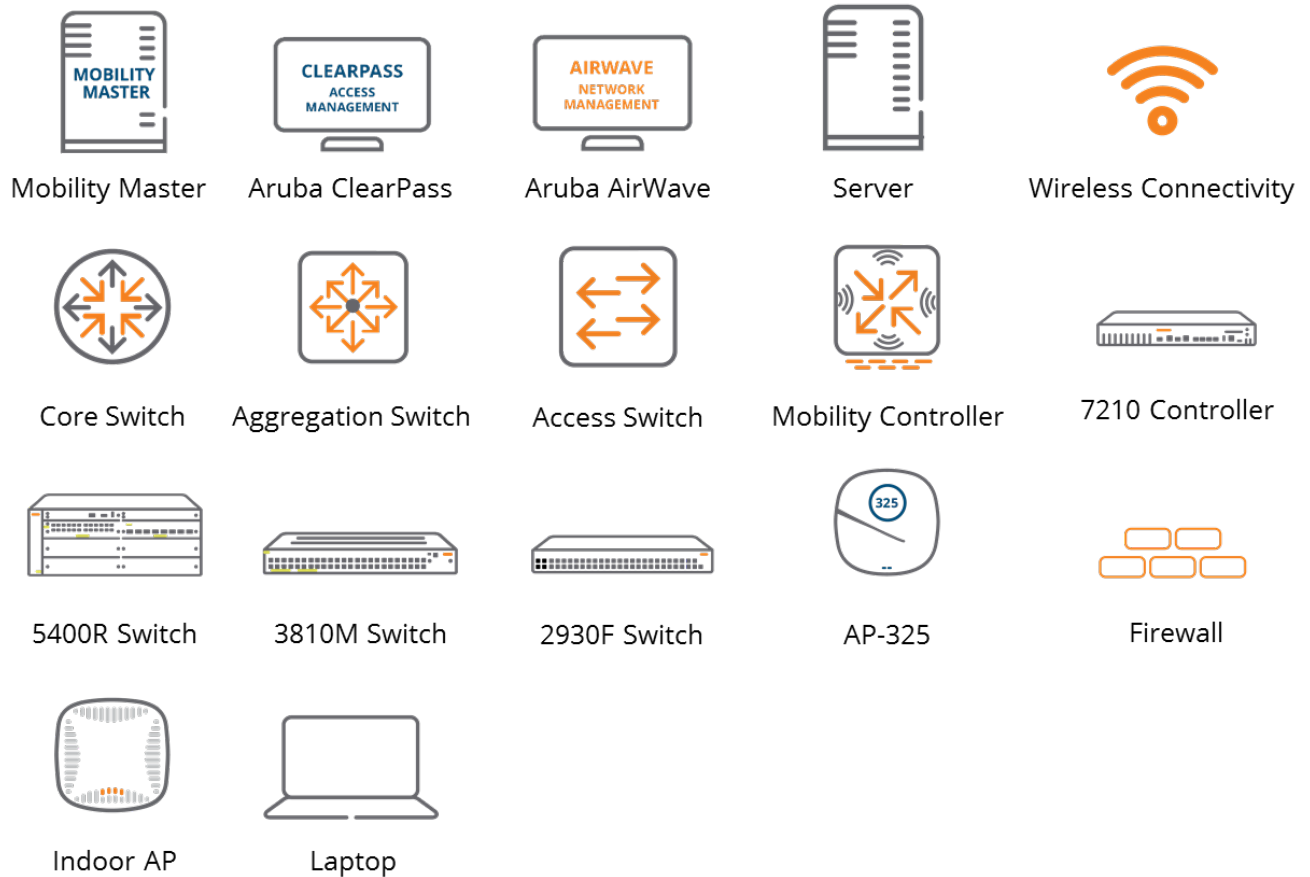


Figure 2 Icon Set

Acronym List

Acronym	Definition
A-MPDU	Aggregated Media Access Control Packet Data Unit
A-MSDU	Aggregated Media Access Control Service Data Unit
AAA	Authentication, Authorization, and Accounting
AAC	AP Anchor Controller
ACR	Advanced Cryptography
AD	Active Directory
AP	Access Point
API	Application Programming Interface
BLMS	Backup Local Management Switch
BYOD	Bring Your Own Device
CoA	Change of Authorization
CLI	Command Line Interface
CPSec	Control Place Security
CPU	Central Processing Unit
DC	Data Center
DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
EAP-PEAP	Extensible Authentication Protocol-Protected EAP
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
FQDN	Fully-qualified Domain Name
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HA	High Availability
HMM	Hardware MM
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IoT	Internet of Things

IP	Internet Protocol
IPsec	Internet Protocol Security
LMS	Local Management Switch
MAC	Media Access Control
MC	Mobility Controller
MCM	Master Controller Mode
MD	Managed Device
MD	Mobility Device
MM	Mobility Master
MM-HW	Mobility Master - Hardware
MM-VA	Mobility Master - Virtual Appliance
MN	Managed Node
NAS	Network Access Server
NAT	Network Address Translation
NBAPI	Northbound Application Programming Interface
PAPI	Proprietary Access Protocol Interface
PEF	Policy Enforcement Firewall
PSK	Pre-shared Key
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RFP	RF Protect
S-AAC	Standby AP Anchor Controller
S-UAC	Standby User Anchor Controller
SfB	Skype for Business
SSID	Service Set Identifier
TOR	Top of the Rack Switch
UAC	User Anchor Controller
UCC	Unified Communications and Collaboration
VIP	Virtual Internet Protocol address
VLAN	Virtual Local Area Network

VM	Virtual Machine
VMC	Virtual MC
VMM	Virtual MM
VPN	Virtual Private Network
VPNC	Virtual Private Network Concentrator
VRRP	Virtual Router Redundancy Protocol
VSF	Virtual Switching Framework
WLAN	Wireless Local Area Network
WPA2-PSK	Wi-Fi Protected Access 2-Pre-Shared Key
XML	Extensible Markup Language
ZTP	Zero-touch Provisioning

Table 3 *Acronym List*

Lab Topology

Recommended Architecture

The *Mobile First Base Designs Lab for ArubaOS 8* VRD will enable readers to quickly setup and configure a state-of-the-art campus network powered by ArubaOS 8. The Aruba campus lab network consists of the following key components:

- Data Center
- Wired LAN (collapsed core design)
 - Core/Aggregation
 - Access
- Demilitarized Zone (DMZ)

The data center (DC) contains all network services and applications along with two fully-redundant virtual mobility masters (VMMs) and four mobility controllers (MC) configured as a cluster.



There are many other possible design scenarios for ArubaOS 8 other than the architecture described above. Please refer to the “Controller Reference Architectures” section of ArubaOS 8 Fundamentals Guide for details.

The wired LAN employs a 2-tier design consisting of dual core switches with VSF (virtual switching framework) redundancy directly connected to aggregation switches for access purposes. The DMZ’s role in the campus topology design is to facilitate a separate domain of guest clients through two MCs, a minimal aggregation layer, and a firewall at the LAN-Internet edge. The topology as a whole utilizes device and link redundancy, hierarchical configuration, and guest traffic isolation through the Multizone feature.

This same network architecture design is frequently used at Aruba for the testing and validation of various network features. It is considered the Aruba base design for ArubaOS 8. Subsequent chapters of this VRD will describe the network design in greater detail including device roles, virtual local area network (VLAN) assignment, redundancy, hierarchical configuration, and guest traffic isolation.

This topology uses existing services running in the corporate server farm. These services include domain controller, Active Directory (AD), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and three Skype for Business (SfB) servers.

The topology depicted below represents the recommended architecture for ArubaOS which has been thoroughly validated by Aruba Technical Marketing Engineering. The actual network which was used for the validation in the TME lab is provided for reference purposes under the Test Lab Network Topology section below.

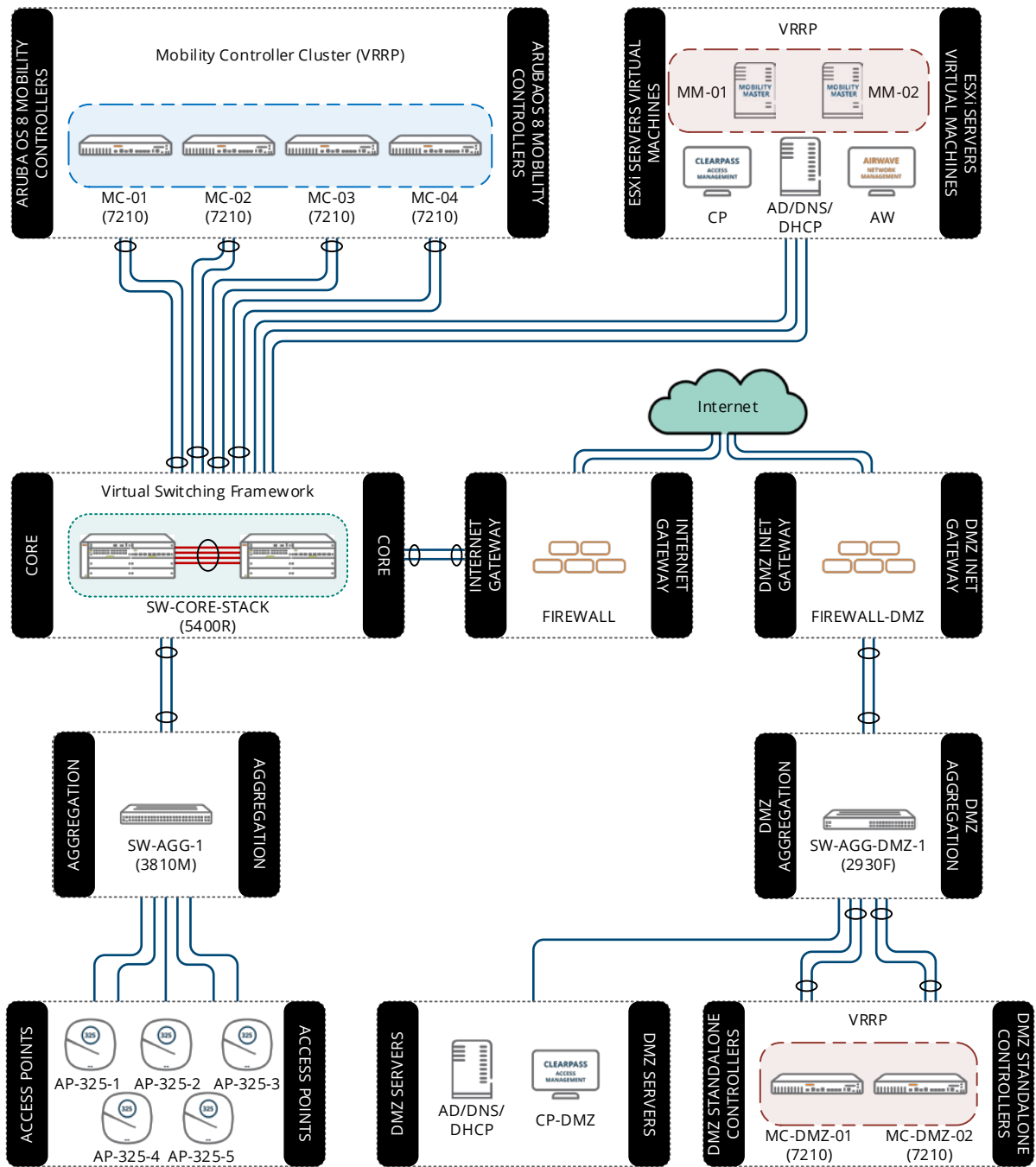


Figure 3 Mobile First Recommended Topology

Test Lab Network Topology

The topology depicted below represents the internal Aruba test network environment which was used to validate the design for the Mobile First Base Designs Lab for ArubaOS 8. The key difference between this topology and the recommended topology depicted above is that instead of separate uplinks from the corporate zone and the DMZ zone to the internet the internal network employs a TOR switch that routes traffic through the internal Aruba corporate network.

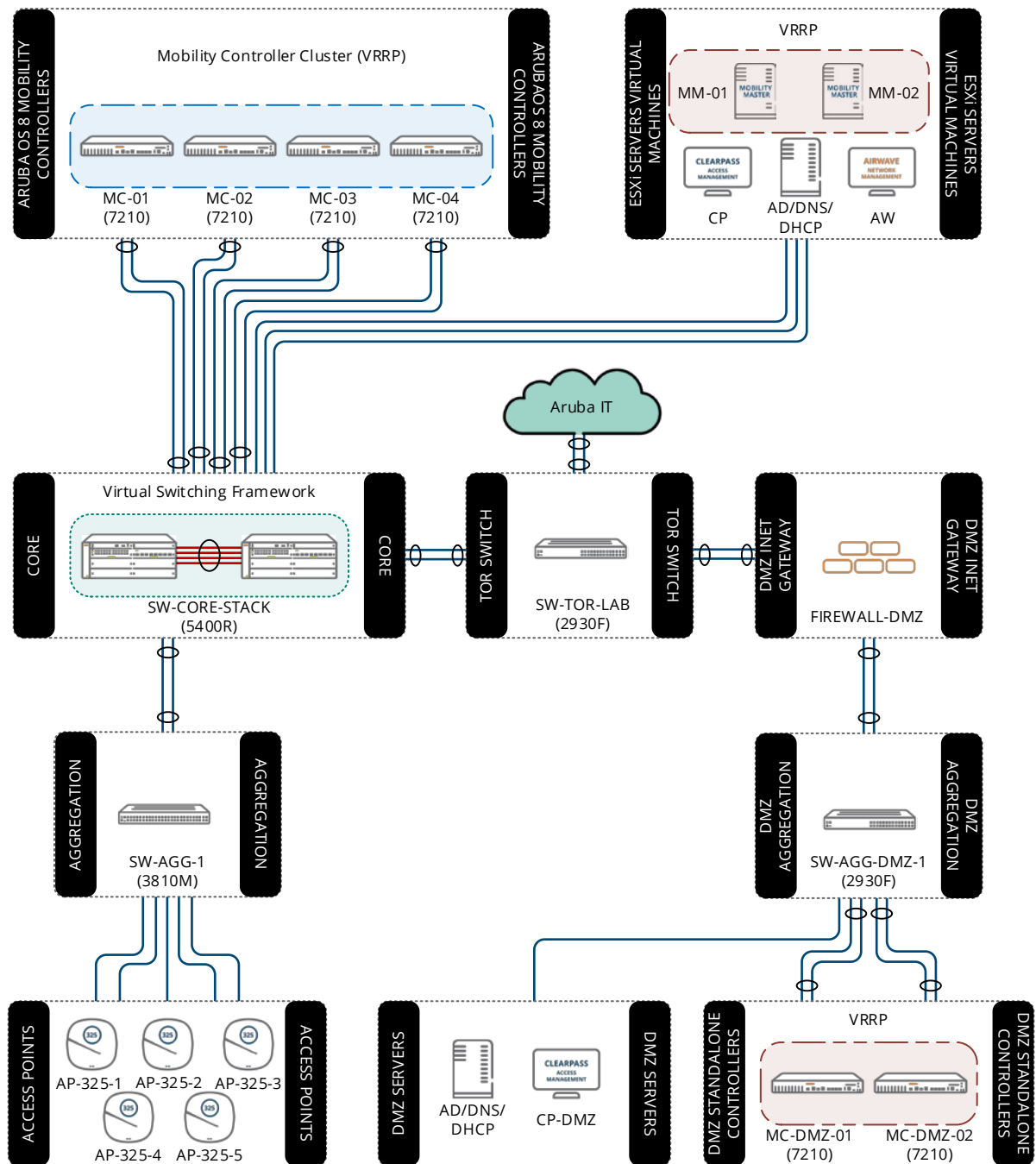


Figure 4 Test Lab Actual Topology

Hierarchical Configuration

ArubaOS 8 Controller Modes

Mobility Master

The concept of the Mobility Master (MM) is new to ArubaOS 8. MMs come in two variations: either Virtual (VMM) or Hardware based (HMM). The MM is designed to run on an x86-based platform as many of the features introduced in ArubaOS 8 require random access memory (RAM), central processing unit (CPU), and storage space that are not supported by physical controllers. The MM must be fully configured by an administrator similar to how a Master controller would be configured in ArubaOS 6. Its primary role in the Mobile First architecture is to serve as the single point of configuration and image management for the network. In addition, the MM can be configured through a Northbound Application Programmable Interface (NBAPI). A VMM can be installed on VMWare, KVM, or Hyper-V depending on which option is the most ideally suited for the environment where it will be deployed.



HMMs and VMMs may alternatively be referred to as MM-HW and MM-VA meaning MM-Hardware and MM-Virtual Appliance, respectively.

The design that was validated for this VRD consists of two MMs which were deployed as virtual machines (VMs) with master-redundancy enabled. Aruba MMs rely on VRRP as their layer 2 redundancy mechanism. The entire configuration hierarchy is automatically synced from the active MM to the standby MM with the exception of any configurations under the device configuration node of the active MM.

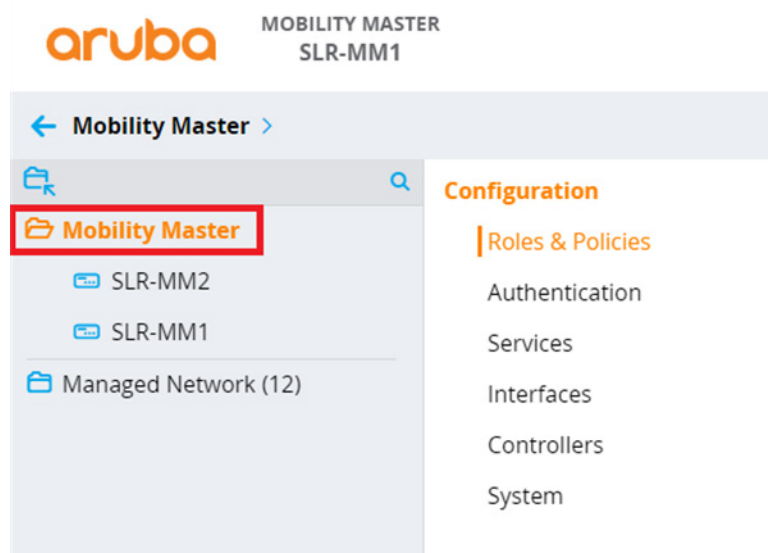


Figure 5 Configuration for All MMs

Configurations that are common to both the active and standby MMs are placed under the **MM** node so that they will be synced. Configurations specific to the Active MM (e.g. IP addresses and VRRP) must be placed individually on its own specific device node. MM services and managed devices cannot be configured from the Standby MM.



Figure 6 Configuration Specific to the Active MM

As soon as VRRP and master redundancy are configured between the active and standby MMs the entire configuration hierarchy is synced. Some of the databases that are synced to the standby MM at periodic intervals when database synchronization is configured on the active MM are listed below:

- WMS Database
- Local User Database
- Global AP Database
- AirGroup Database
- License Database
- CPsec Database

The synchronization interval is specified as part of the database synchronization configuration. The database synchronization interval is configurable. As a best practice Aruba recommends configuring the interval for of 10 minutes and it should never be set for more than 20 minutes.

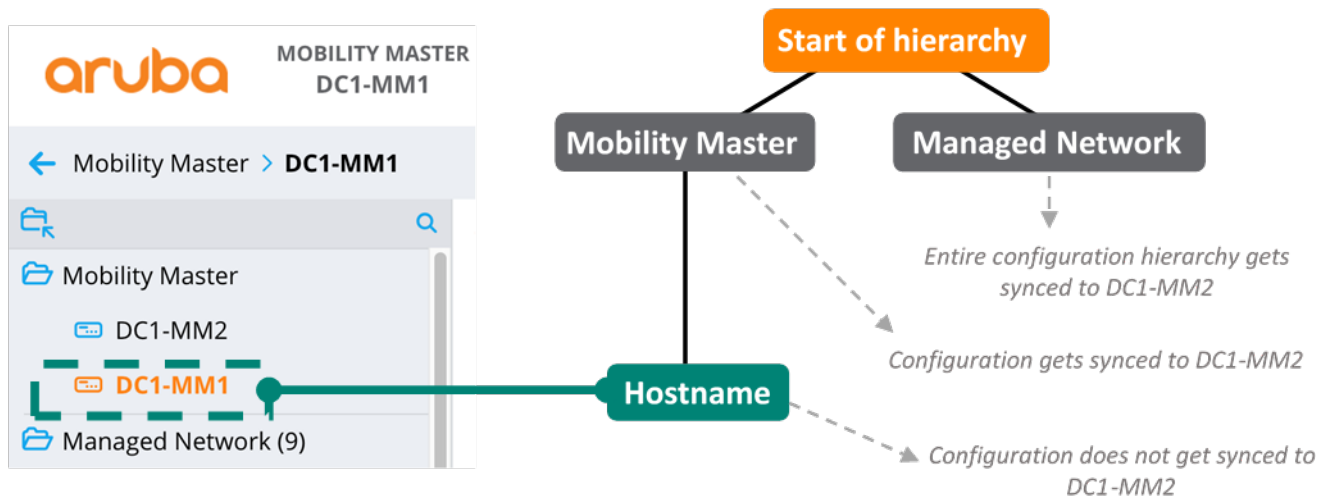


Figure 7 Database Synchronization

Once the active and standby MMs have performed their initial synchronization and reached a stable state, any incremental configuration change that is committed and saved on the active MM results in a configuration sync with the standby MM.

The exception to this behavior is any change made on the device configuration node of the active MM (i.e. /mynode). These changes are not synced to the standby MM. The standby MM contains its own version of the device configuration so any desired changes must be made directly on its corresponding device configuration node (i.e. /mynode on the standby MM). Configuration changes for other nodes in the hierarchy are not permitted on the standby MM.

Mobility Controller

The concept of the Mobility Controller or “MC” is also new to ArubaOS 8. An MC, in the past, has also been known as Managed Node (MN), Managed Device (MD), or Mobility Device (MD) in some Aruba documentation. An MC is similar to a Branch controller in ArubaOS 6 in the sense that it can be adopted using zero touch provisioning (ZTP) and Aruba Activate. The last port of an MC is enabled as a DHCP client on VLAN 4094 in its factory default configuration.



MMs cannot adopt an MC using DHCP Option 43 since MM certificate distribution is not supported with DHCP Options. VMCs used as VPNCs do not support ZTP when the MM is behind the VPNC due to the lack of a Trusted Platform Module (TPM). ZTP requires certificate-based authentication for the initial connection to the MM.

Unlike the ArubaOS 6 Local controllers, MCs can be fully managed by an MM or Mobility Controller Master (MCM). In addition, unlike ArubaOS 6 Branch controllers, an administrator can configure every feature of an MC. All 70xx series controllers and 72xx series controllers are shipped as MCs. ArubaOS 8 also supports Virtual MCs (VMC). A VMC can be deployed either on VMWare, KVM, or Hyper-V. MCs can be configured as Virtual Private Network Concentrators (VPNCs).

ArubaOS 8 Enhancements

ArubaOS 8 introduces true ZTP for all deployment modes as well as the concept of hierarchical configuration. New campus or branch controllers can discover the MM using DHCP options or Aruba Activate and receive their entire configuration from the MM. Regardless of the scale of controllers being managed the MM acts as a single touch point for the entire deployment.

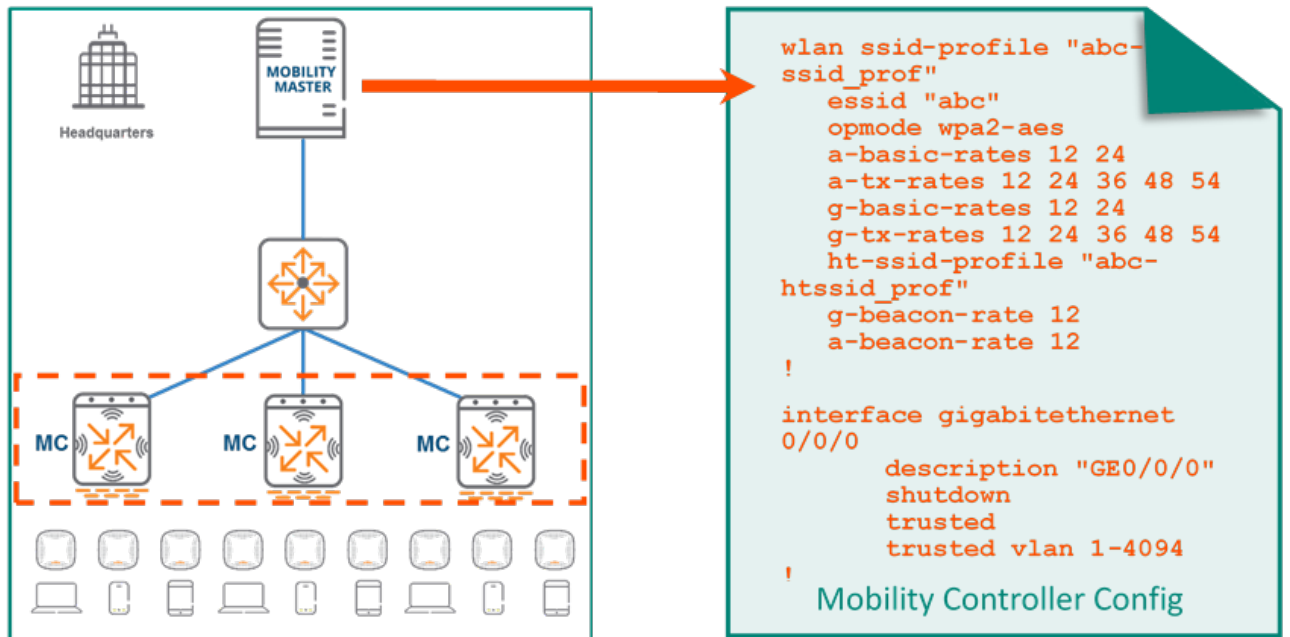


Figure 8 AOS 8 Configuration

Hierarchical configuration allows configuration nodes to be created on the MM which contain common configurations for a particular region, campus, or building. Once a controller is whitelisted under a configuration node, a device-level configuration can be added on the device configuration node. When the MC contacts the MM for the first time, the group level configuration is merged with the device level configuration and then pushed down to the MC.

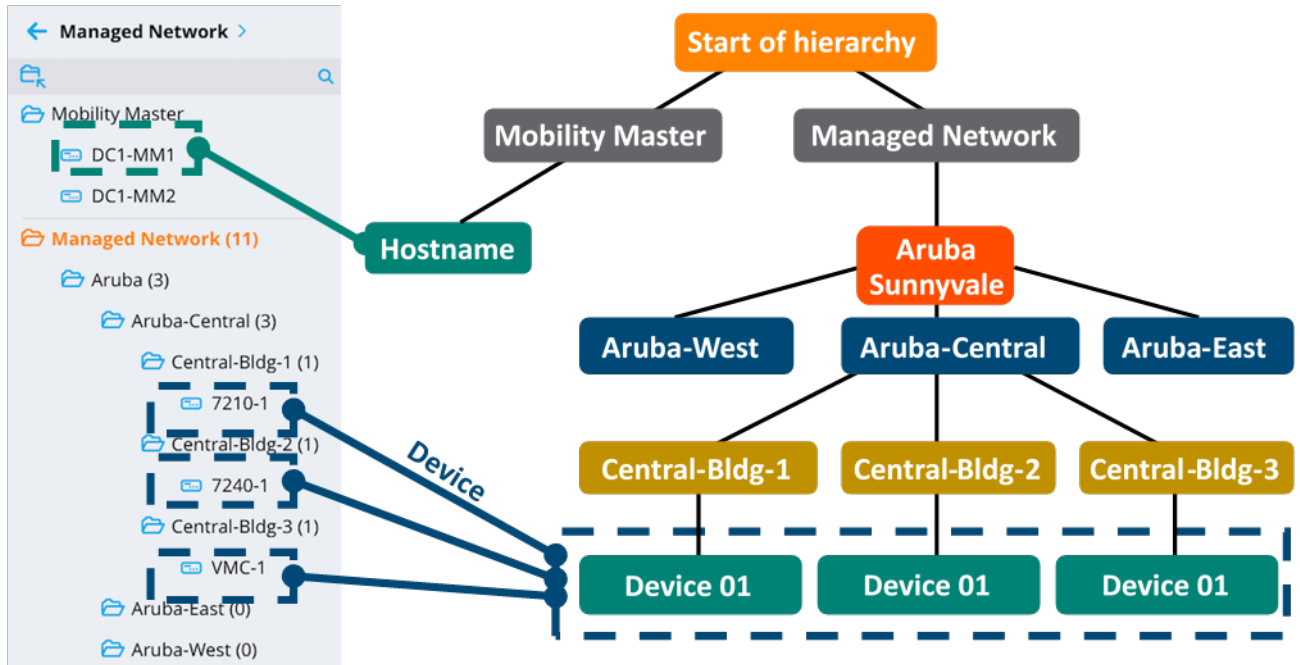


Figure 9 Configuration Hierarchy

The hierarchical configuration model has system-defined as well as user-defined configuration nodes.

System Nodes

System level nodes are present on GUI of the MM by default and cannot be deleted. The system nodes are as follows:

- **MM** – In the case of redundant MMs the configuration defined at this node is common for both active and standby MMs
- **Hostname (of MM)** – Holds configuration for the actual MM
- **Managed Network** – Hierarchy under which all the user-defined nodes are created and controllers are configured

User Nodes

User-defined nodes are created by administrators under the **Managed Network** system node. A node hierarchy can be created under this node where the upper nodes hold common configuration for all controllers. The configuration becomes more specific (based on region, campus, or building) at lower levels of the hierarchy. The device nodes are defined at the very bottom. The following examples demonstrate hierarchical group and device node definitions:

Managed Network > Aruba > Aruba-Central > **Central-Bldg-2** >

Figure 10 Group Node Example

Managed Network > Aruba > Aruba-Central > Central-Bldg-2 > **7240-1**

Figure 11 Device Node Example

Up to four nested child nodes can be created under the Managed Network node. For example:

Managed Network > Aruba > Aruba-West > Campus1 > **Building-2**

Figure 12 Four Nested Child Nodes

Numerous child nodes can be created under the same parent node. In addition, child nodes can be freely moved to other nodes in the hierarchy as well as cloned from other nodes under the same parent node.

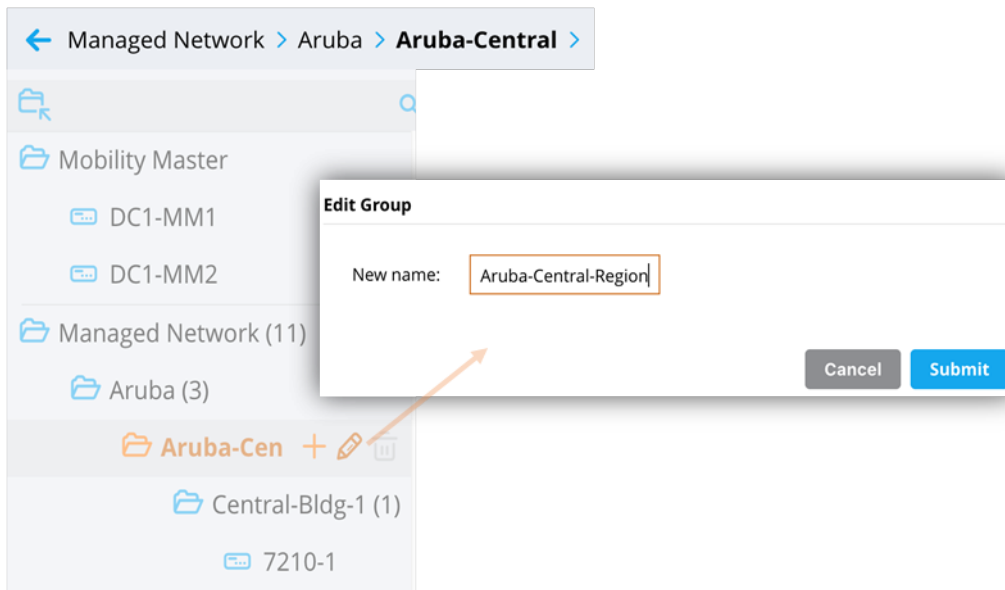


Figure 13 Renaming a Node

Configuration Inheritance

When an MC initially contacts the MM, it will merge the configuration at the device node with configurations from higher up in the hierarchy all the way up to the **Managed Network** node.

If there is a conflict or overlap in configuration on any node the configuration defined on the lower nodes will take precedence over the configuration on the higher nodes when pushing down the final configuration. The example below shows how a controller inherits its final configuration from the MM:

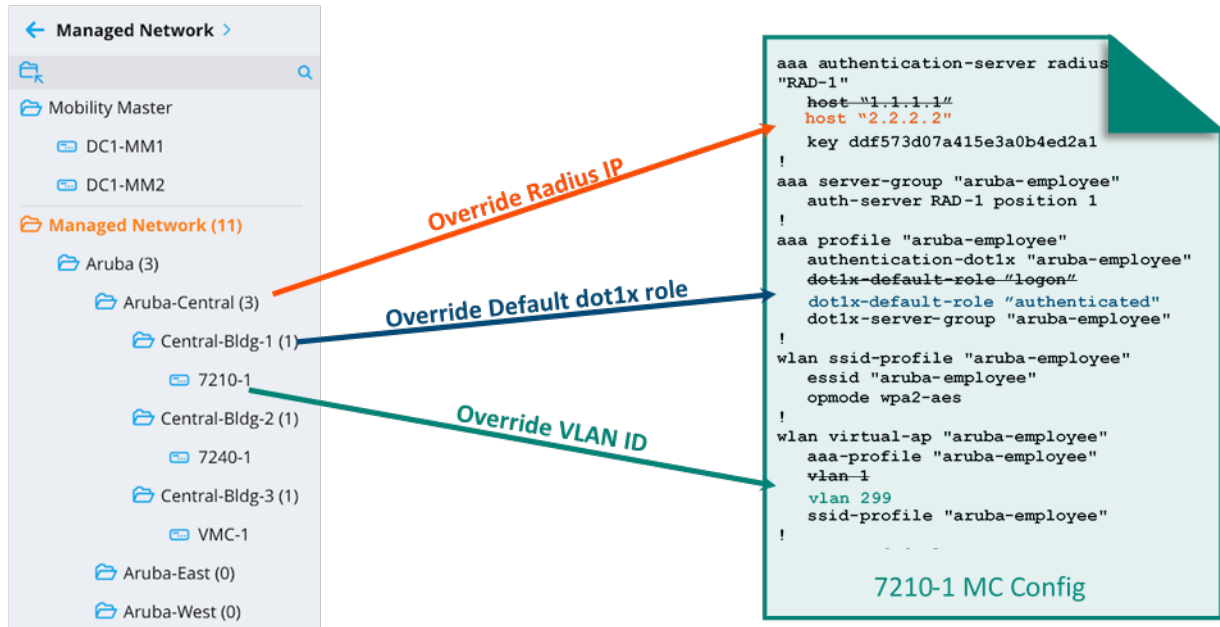


Figure 14 MM Configuration Inheritance

In the example above the initial configuration is created on the user-defined **Aruba** node which will be common to all the controllers in the organization. Since the **Aruba-Central** Node is farther down the hierarchy it will receive its initial configuration from the Aruba node and then override the RADIUS IP address. Similarly, the **Central-Bldg-1** node and the **7210-1** device node will override the dot1x role and the VLAN ID defined in the original configuration, respectively. The following figures display some of the key elements which were configured using the **Managed Network > Aruba** path:

Server Group > aruba-employee		Servers	
NAME	TYPE	IP ADDRESS	TRIM FQDN
RAD-1	Radius	1.1.1.1	--

Figure 15 RADIUS Server RAD-1 with RADIUS IP "1.1.1.1"



Please refer to the [Configuration Overrides](#) section for a description of items which cannot be overridden.

AAA Profile: aruba-employee

Initial role:

MAC authentication default role:

● 802.1x authentication default role:

Figure 16 802.1X Default Role of Logon

The presence of the blue dot next to a configuration parameter indicates the value was overridden such as in the case of a change to the configuration inherited from the parent node or a blank value that was replaced. Clicking on the blue dot displays additional details about the change and provides the option to either remove or retain the override.

aruba-employee **General**

VLAN:

Figure 17 VLAN "1"

In the figure below the **Aruba-Central** node inherited this configuration, however the IP of the RADIUS server **RAD-1** was changed to "2.2.2.2":

Server Group > aruba-employee > RAD-1 **Server Options**

Name:

● IP address / hostname:

Figure 18 RADIUS Server IP Override

On the **Central-Bldg-1** node father down, the presence of the blue dot indicates that the default 802.1X role in the authentication, authorization, and accounting (AAA) profile was changed to "authenticated" and the configuration received from the parent node was overridden. **Managed Network > Aruba > Aruba-Central > Central-Bldg-1:**

AAA Profile: aruba-employee

Initial role:

MAC authentication default role:

● 802.1x authentication default role:

Figure 19 Authentication Default Role Override

Lastly, the VLAN applied to the Virtual AP profile “aruba-employee” on the device node **7210-1** was changed to “299”. **Managed Network > Aruba > Aruba-Central > Central-Bldg-1 > 7210-1:**

Virtual AP profile: aruba-employee

Broadcast/Multicast

General

Virtual AP enable:

● VLAN:

Figure 20 VLAN Changed to 299

When the 7210 controller assigned to the **Central-Bldg-1** node contacts the MM for the first time, its inherited configuration will result in the following changes:

	Original Configuration	Inherited Configuration
RADIUS Server IP	1.1.1.1	2.2.2.2
802.1X Default Role	logon	authenticated
VLAN	1	299

Table 4 Summary of Inherited Configuration Changes

Node Level Administration

Hierarchical configuration makes it possible to create node-level administration accounts on an MM. Network administrators can fully manage configuration for controllers at and below the configuration nodes that they have the necessary permission to access such as at a region, campus, or building level without affecting controllers elsewhere in the global hierarchy. This feature ensures that any undesirable configuration changes made at local sites are contained and do not affect the entire organization.

Proof-of-concept testing is another use case where custom ArubaOS builds and features need to be lab tested before bringing them into production. In such a scenario, test configuration nodes could be created along with node-level administration accounts. Since the nodes are created in a sandbox environment, testing may be freely performed without creating any undesirable effects higher up in the configuration hierarchy.

Licensing Pools

Licensing in ArubaOS 8 is managed centrally from the MM and the global license pool will be used by default for all controllers under its management. However, if specific license pools need to be dedicated, such as for a particular region, then custom license pools must be created on the MM with the appropriate hierarchical node and license counts definitions.

Configuration Best Practices

Prior to deploying controllers there should be a defined plan on the configuration hierarchy for a network will look like. The following sections provides guidance for developing a configuration and deployment plan.

Node Hierarchy Design

There are multiple approaches to implementing a hierarchical design:

- A configuration hierarchy is typically created based on geographical segmentation of controllers. If an organization has multiple offices across a country then it makes sense to create configuration nodes for each region such as East, Central, and West. Each of these regions in turn may have multiple campuses, buildings, and devices which each have their own configuration node.
- An alternative way of organizing a hierarchy could be based on the type of services offered such as campus and remote with regional variations at the bottom of the tree.

Hierarchical configurations should be designed so that that configurations that are common to the organization reside on the higher level nodes. The rest of the configuration will be inherited by the lower nodes of the hierarchy as network requirements become more specific. E.g., a named VLAN can be defined at a higher level of the hierarchy and then assigned with specific VLAN IDs at the lower levels. Finally, configurations specific to individual controllers such as IP addresses, physical and virtual interfaces, and cluster membership are configured at the device level nodes. As a best practice, all configurations that are dependent on a single node should be always be defined e.g., defining VLAN ID and VLAN interface parameters together in a common node.

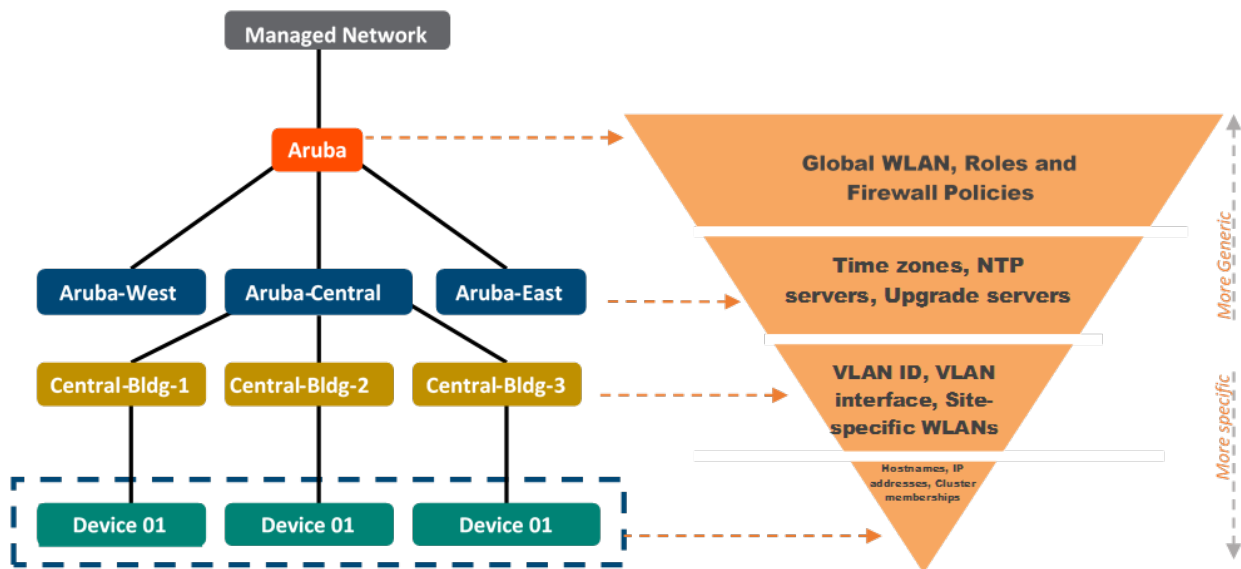


Figure 21 Node Hierarchy Design

Configuration Overrides

Generally, a configuration that is inherited from higher level nodes cannot be deleted, however it can be overridden on the lower level nodes. However, there are certain configuration parameters that cannot be overridden at the lower level nodes. These parameters include the following:

- Net destinations
- IP access lists
- User roles
- AAA server groups
- AAA user derivation rules



Numerous overrides across many hierarchy levels should be avoided as it can make troubleshooting challenging.

Depth of Hierarchy

Up to four nested child nodes can be created under the **Managed Network** node. However, it is recommended to create only as many nested nodes that are needed for purposes of configuration management simplification.

The Managed Network Node

As a best practice Aruba recommends defining configurations at a node below the Managed Network node and not on the Managed Network node itself. This is done to allow for sufficient network growth and scalability while simultaneously maintaining a separate configuration hierarchy for new sites. Configuration on the Managed Network node should be kept as minimal as possible in order to prevent the spread of issues related to misconfiguration across every other node in the hierarchy.



Aruba strongly discourages placing any configuration on the **/md (Managed Network)** node under any circumstances. Modifying configurations at this level will permanently alter the configuration for every child node without any ability to determine the default settings. Configurations should always begin a level below the **Managed Network** node.

Sites can be differentiated either physically or by type. In the example below, if the organization “Aruba” acquired another company “Network-Co”, then we could simply define a new configuration node under **Managed Network** called **Network-Co** parallel to the **Aruba Sunnyvale** node.

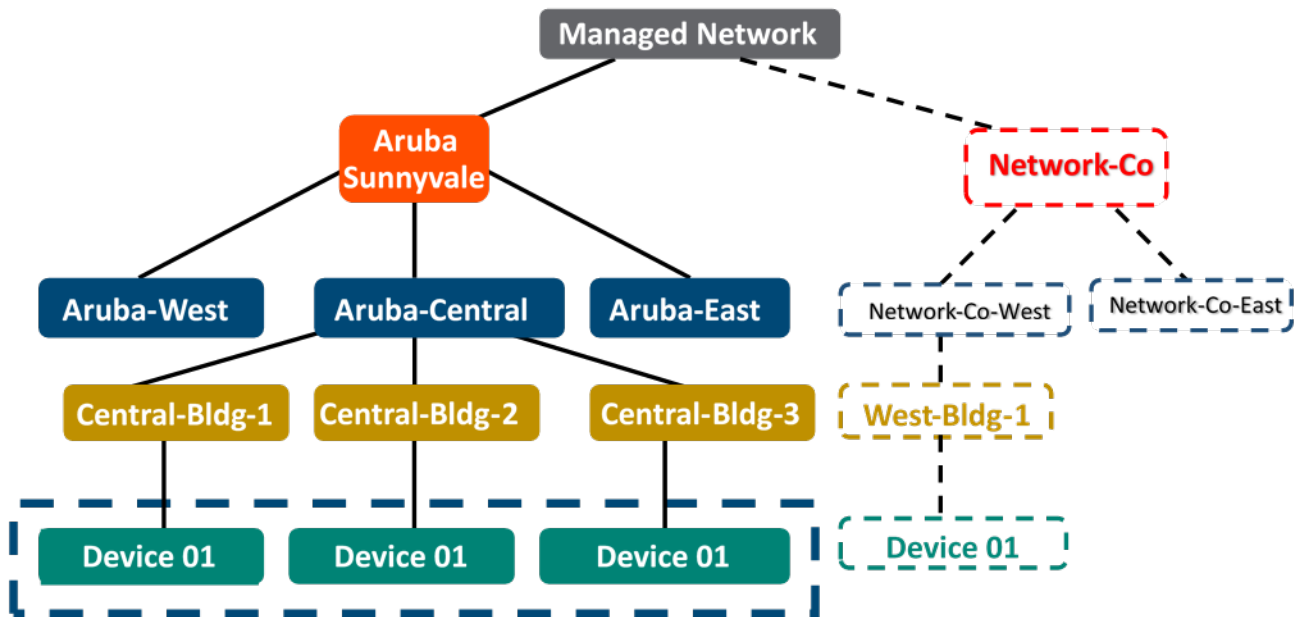


Figure 22 Managed Network Node Hierarchy

Configuration Notes

- When manually bringing up MCs it is important to ensure that they have been whitelisted on the MM under the appropriate configuration node
- When using ZTP to bring up MCs it is critical to ensure that the correct configuration node and MM MAC address are configured on Activate.
- Verify that the MM has learned about the MCs from Activate and whitelisted them under the configuration nodes that were specified in the Activate provisioning rule
- When specifying the MAC address of the MM for establishing an IPsec connection during initial configuration of controllers, always ensure that the management port hardware MAC address is used for a VMM and the hardware MAC address is used for an HMM
- When the MM registers with Activate, the correct MAC address is automatically populated. If controllers are using ZTP to contact Activate and register with the MM, identify the MAC address of the MM and select it from the dropdown list when configuring the provisioning rule on Activate

Edit Rule

Input for Rule

Rule Type: Provisioning Rule

Parent Folder: [Folder Name] ▼

Provision Type: Managed Device to Master Controller

Redundancy Level: L2 ▼

Config Node Path: /md/poc

Master Controller: 00:50:56:85:65:22 ▼

Master Controller IP:

Backup Master Controller:

VPN Concentrator MAC:

VPN Concentrator IP:

Backup VPN Concentrator MAC:

Country Code:

Rule Name:

Done Cancel Re-C

00:0C:29: [blurred]
 00:0C:29: [blurred]
 00:0C:29: [blurred]
 00:0C:29: [blurred]
 00:0C:29: [blurred]
 00:1A:1E: [blurred]
 00:50:56: [blurred]
 00:50:56: [blurred]
 00:50:56: [blurred]
00:50:56:85:65:22
 00:50:56: [blurred]
 00:50:56: [blurred]
 00:50:56: [blurred]
 00:50:56: [blurred]
 00:50:56: [blurred]
 00:50:56: [blurred]

Figure 23 *Selecting the MM MAC Address*

Tunneling and Control Plane Security

In most ArubaOS 8 topologies campus APs typically operate in one of two modes when communicating with their MC:

- Tunnel Mode
- Decrypt Tunnel Mode

The advantage to both these modes is that the user VLANs reside on the controller and do not have to be managed at the edge. Additional VLANs can be added to the core switch where the MC uplink is connected if necessary. There is no need to add them to the edge switch where the APs terminate. Both of these operating modes simplify network design and allow for flexibility in terminating users.



The Mobile First architecture that has been validated and described in this document uses Tunnel Mode.

Tunnel Mode

When operating in the Tunnel forwarding mode, the AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames, and EAPOL frames over a Generic Routing Encapsulation (GRE) tunnel to the MC for processing. The MC then removes or adds the GRE headers, decrypts or encrypts 802.11 frames, and applies firewall rules to the user traffic as usual.

To achieve maximum performance benefits with Tunnel Mode, end-to-end jumbo frame support should be enabled on a wired switch due to the increased aggregation introduced with the IEEE 802.11ac standard. Using Control Plane Security (CPSec) in Tunnel Mode is not mandatory. The majority of production deployments utilize Tunnel Mode for AP forwarding where the AP sends 802.11 traffic to the controller. Control and data plane traffic between the AP and the MC is always encrypted. Aruba recommends using Tunnel Mode with jumbo frames as a best practice as the majority of traffic fits in a standard Ethernet frame and no special handling is required on the wired network to achieve maximum aggregate performance.

Without end-to-end jumbo frames on the wired network, 802.11ac networks can experience significant performance degradation in some cases. Although, it should be noted that this adverse impact to performance is only noticed when the peak network performance is measured during technology demonstrations. The day-to-day operations in real world production networks are typically unaffected without jumbo frames turned on.



Aruba recommends enabling jumbo frames end-to-end as a best practice.

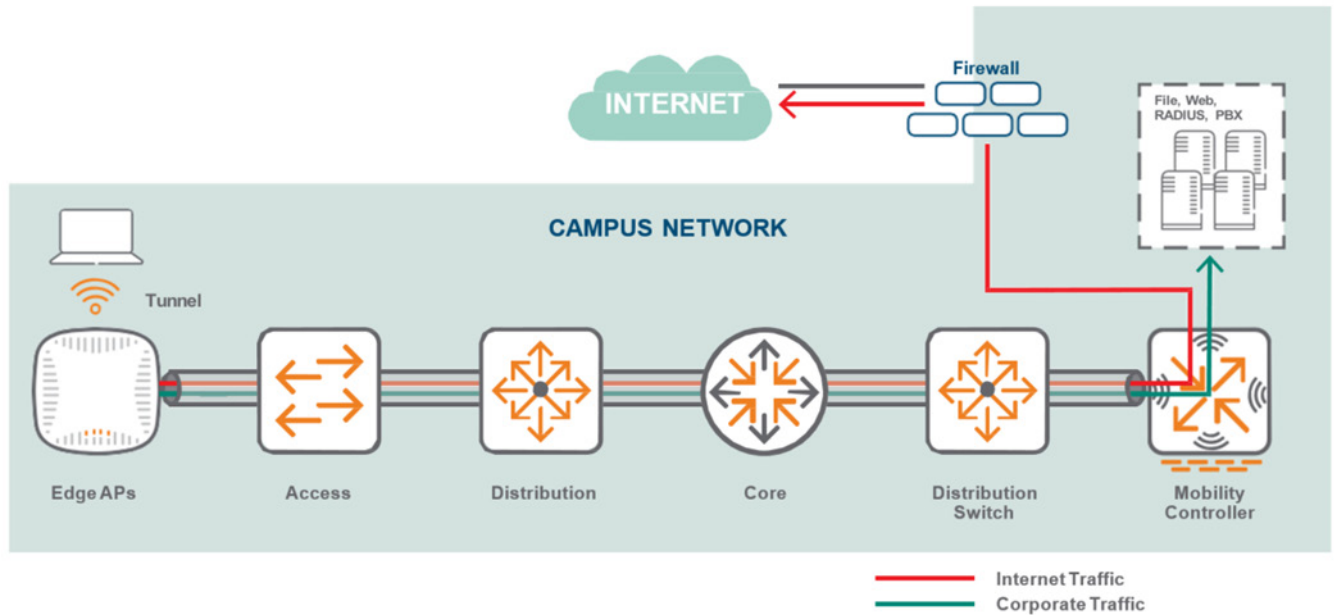


Figure 24 Tunnel Forwarding Mode

Decrypt-Tunnel Mode

Decrypt-tunnel mode allows an AP-client pair to take full advantage of Aggregated-Media Access Control (MAC) Service Data Units (A-MSDUs) and Aggregated-MAC Packet Data Units (A-MPDUs) without requiring the wired network to transport jumbo frames. APs perform decryption and de-aggregation on themselves locally. It is mandatory to enable control plane security (CPSec) between APs and Controllers when using Decrypt-tunnel Mode.



Decrypt-tunnel Mode does not provide end-to-end encryption. Only the control plane traffic between APs and MCs is encrypted in Decrypt-tunnel Mode.

In Decrypt-tunnel mode the AP acts as a bridge between clients and the controller in addition to performing encryption and decryption. The MC still acts as the aggregation point for terminating data traffic. This allows the AP-Client pair to take advantage of A-MSDU and A-MPDU on the WLAN radio side without requiring the wired network to transport the jumbo frames since the AP performs all assembly aggregation and de-aggregation locally. The payload is then sent to the controller for firewall processing and L2/L3 forwarding.

Decrypt-tunnel Mode is functionally equivalent to Tunnel Mode with jumbo frames enabled and is typically used for technology demonstrations. It is important to keep in mind that the AP wireless chipset performs cryptography for up to 50 clients which is offloaded to the AP hardware. Scenarios involving more than 50 clients will likely experience minor performance degradation due to this offload process.

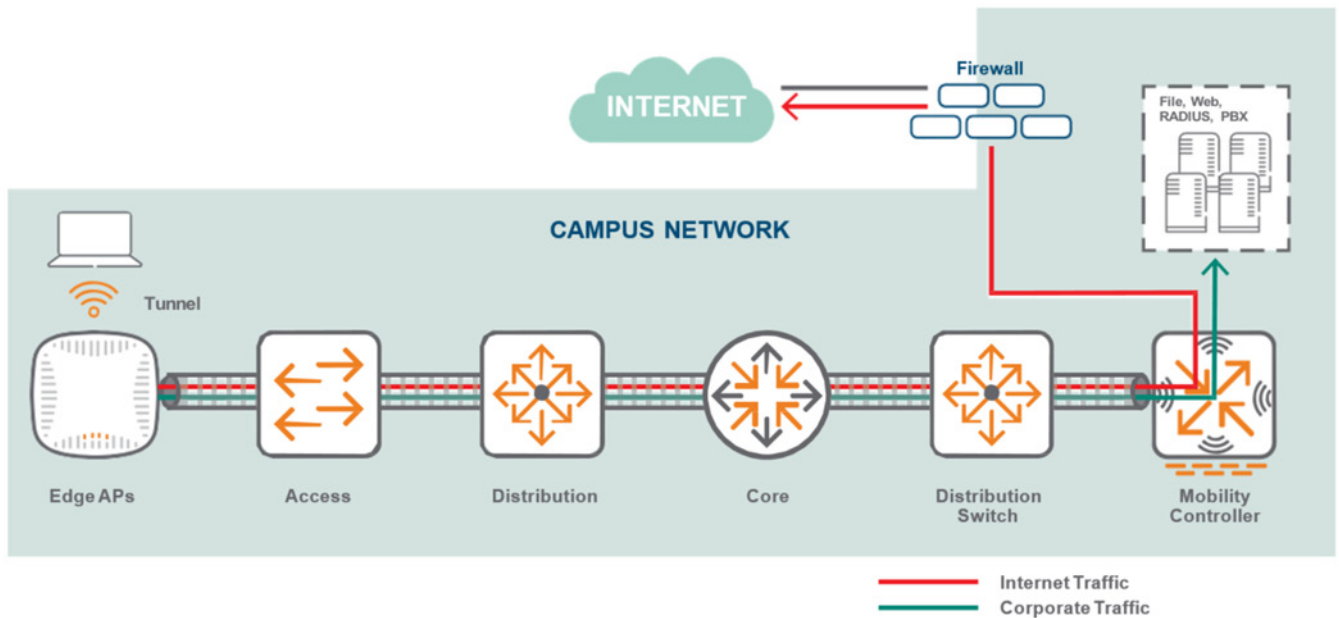


Figure 25 Decrypt Tunnel Forwarding Mode

Control Plane Security

The CPSec feature has two main functions:

1. Securing the control channel between Aruba MCs and their attached APs
2. Preventing unauthorized APs from joining the Aruba WLAN network

The aforementioned goals are achieved in the following manner:

The control traffic transported using Proprietary Access Protocol Interface (PAPI) is secured using a certificate-based Internet Protocol Security (IPsec) tunnel in transport mode

A CPSec whitelist database holds the list of APs authorized to connect to the Aruba controllers and join the WLAN network

Since CPSec is enabled by default, the MM certifies its MCs using its generated factory certificate after booting up. MCs in turn certify their APs by signing their factory default certificates. Once the APs are authorized through the CPSec whitelist and enter the *certified-factory-cert* state they will initiate secure PAPI (UDP 8209 inside IPsec) communication with the controller, synchronize their firmware, and download their configuration.

Boot Process with Control Plane Security

The figure below illustrates the steps involved in the campus AP boot process with CPsec:

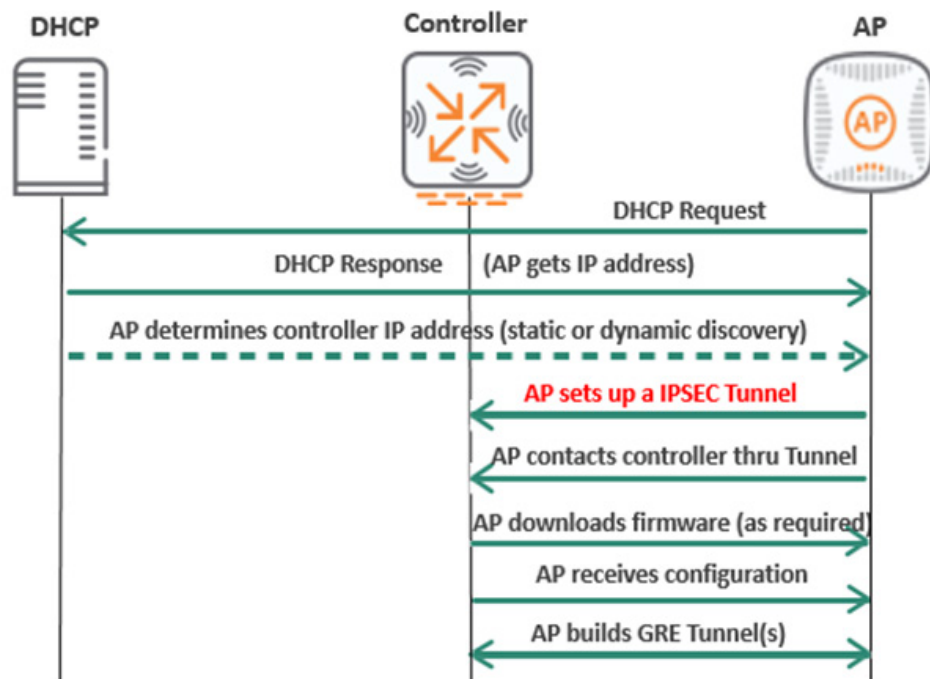


Figure 26 Boot Process with CPsec

Clustering

Clustering is one of the key features introduced in ArubaOS 8 and was specifically designed to capitalize on the MM architecture and deliver maximum value for mission-critical networks. Clustering was developed to achieve the following objectives:

- **Seamless Campus Roaming** - Clients in a single large layer 2 domain will associate and stay anchored to a single MC as they roam. Users will maintain the same subnet and IP address regardless even if they roam across APs which are anchored to different controllers. This enables mobility without compromising or sacrificing performance
- **Stateful Client Failover** - User traffic will remain uninterrupted and high value sessions will be preserved in the event of a cluster member failure. Clients will not be required to re-authenticate and there will be no adverse impact to performance. The impact to performance will be mitigated to such an extent that users will not notice any degradation in their performance and they will have no knowledge that a failure has even occurred regardless of the applications they are currently utilizing
- **Access Point and Client Load Balancing** - APs and users are automatically load balanced across controllers that are members of the cluster. This process prevents any one MC from being disproportionately loaded in order to deliver and maintain optimal network performance as well as to preserve capacity across all cluster members for new client associations
- **Live Upgrade** - Aruba allows customers to perform in-service cluster upgrades which allow improvements to be implemented without affecting performance while the network remains fully operational. The Live Upgrade feature allows upgrades to be completely automated. This is a key feature for customers with mission-critical networks that must remain operational 24/7. Live upgrades can only be performed on MCs in a cluster and the APs attached to them

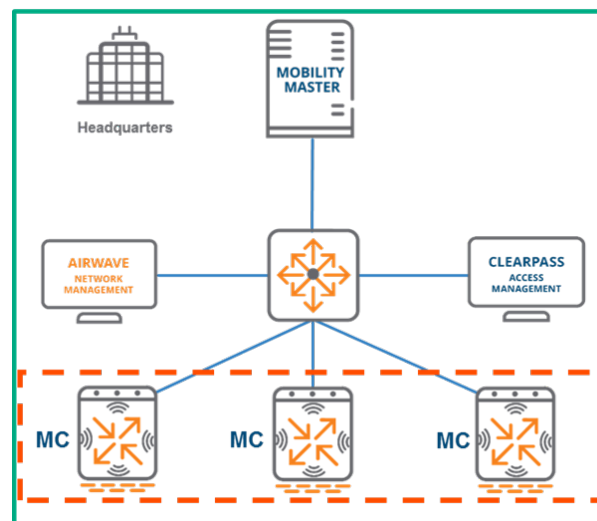


Figure 27 Typical MC Cluster Architecture

Benefits and Considerations

Clustering is a key feature of ArubaOS 8 however it cannot be enabled for all devices. Only MCs under management of an MM can form a cluster. MMs themselves however cannot become a member of a cluster with another MM nor with MCs. MMs strictly function as management devices for MCs in a cluster. While the redundancy options for an MM environment include both clustering as well as High Availability (HA) with AP Fast Failover, these are mutually exclusive features. One or the other must be chosen as they cannot both be concurrently operational.



All MCs in a cluster need to run the same software version so that APs that failover to a new controller will not inadvertently upgrade to a new version.

It should be noted that clustering is not supported by Standalone controllers. If Standalone controllers must be used then their primary redundancy mechanism is HA. Clustering and all of its constituent features are supported for both Campus Access Points, Remote Access Points, and meshed Access Points without requiring any additional licenses. The controller models which support clustering include the 72xx family, the 70xx family, and VMCs.



Publicly-routable addresses are required to enable clustering with RAPs.

The cluster capacity for each product line is detailed in the table below:

Product Family	Devices per Cluster
72xx	12
70xx	4
Virtual	4

Table 5 Cluster Capacity by Product Family

While it is technically possible to combine 72xx and 70xx devices in the same cluster doing so is strongly discouraged as a long term deployment option. Such a scenario is acceptable as a temporary migration strategy however as a best practice cluster devices should always be homogeneous. If different controller models are clustered together then all controller scalability limits will be downgraded to the capabilities of the lowest controller model. E.g., if a cluster was created with two 7240 controllers and one 7210 controller then the cluster's scalability capacity will be limited to that of three 7210 controllers.



Virtual and hardware controllers cannot be combined in a cluster under any circumstances.

The figure below depicts the dashboard view for a cluster:

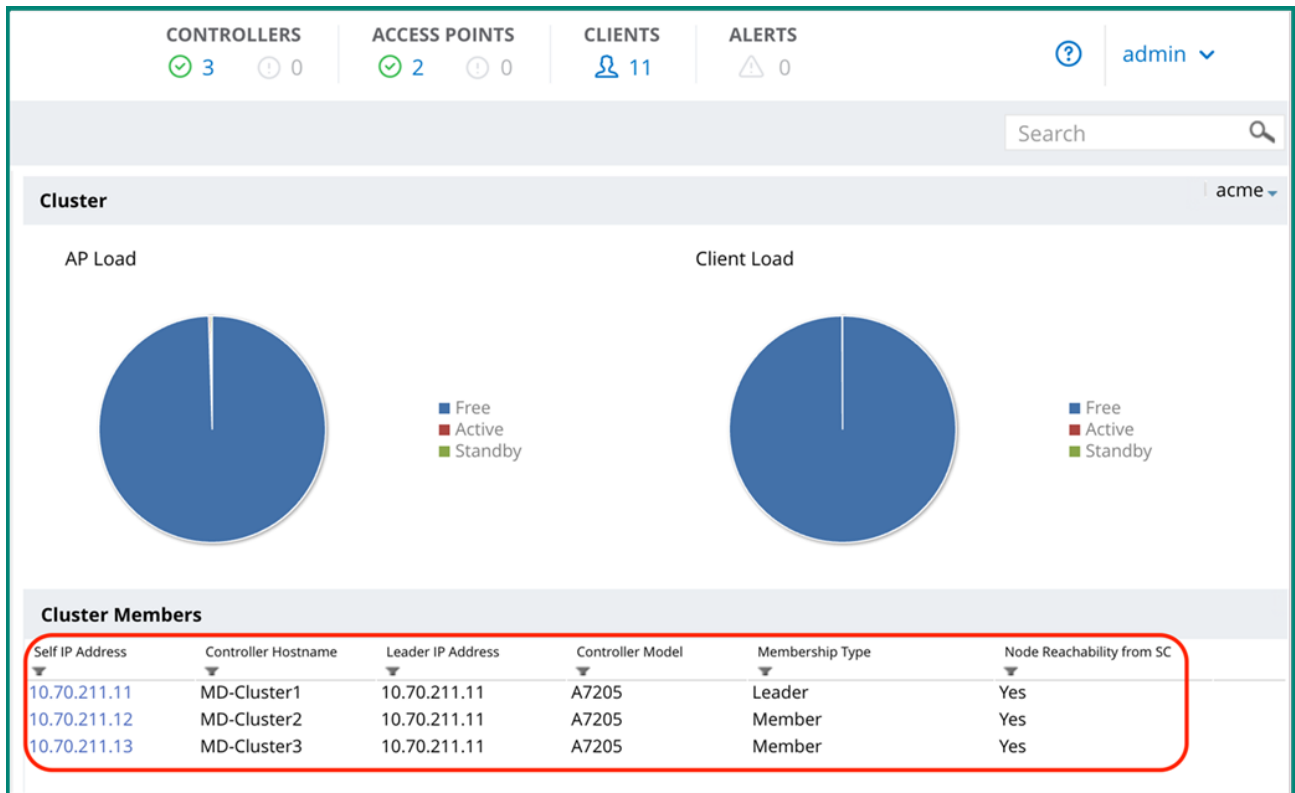


Figure 28 MM Cluster Dashboard

The view above can be accessed through the GUI by navigating to the **Cluster** tab of the main dashboard. Key statistics about a cluster can be seen under this tab including the number of controllers, APs and clients in the cluster under management by the MM as well as the current AP and client loads of the cluster members. The **Cluster Members** section at the bottom displays key statistics pertaining to the MC which are members of the cluster including their IP address, model, and which device is acting as the current cluster leader.

Local Management Switch

In multi-controller networks, each controller acts as a local management switch (LMS) by terminating user traffic from the APs, processing, and forwarding the traffic to the wired network. An LMS and a backup local management switch (BLMS) are the primary and secondary connection points for an AP. APs rely on heartbeat timeouts with the LMS controller to failover to a preconfigured BLMS controller.

When controllers are in separate L3 networks, Virtual Router Redundancy Protocol (VRRP) cannot be used for redundancy. In such a case, the LMS and BLMS should be used for redundancy.

In the most basic scenario of two L3 separated controllers:

- The AP finds aruba-master and obtains the LMS and BLMS IPs as part of its configuration
- The AP terminates on the LMS controller
- If the LMS controller fails, eight consecutive missed heartbeats will trigger an AP failover
- The AP comes up on the BLMS

Another scenario could be an AP terminated on an LMS that is a cluster of controllers. An AP finds the aruba-master and obtains the IP addresses of its LMS and BLMS as part of its configuration. If the LMS is located in a cluster of controllers and the LMS fails, any APs terminated on that LMS will attempt to failover to the other members of the cluster. The AP will only failover to its BLMS if all of the other members in the cluster have failed. The BLMS could either be a single controller or a member of a cluster.

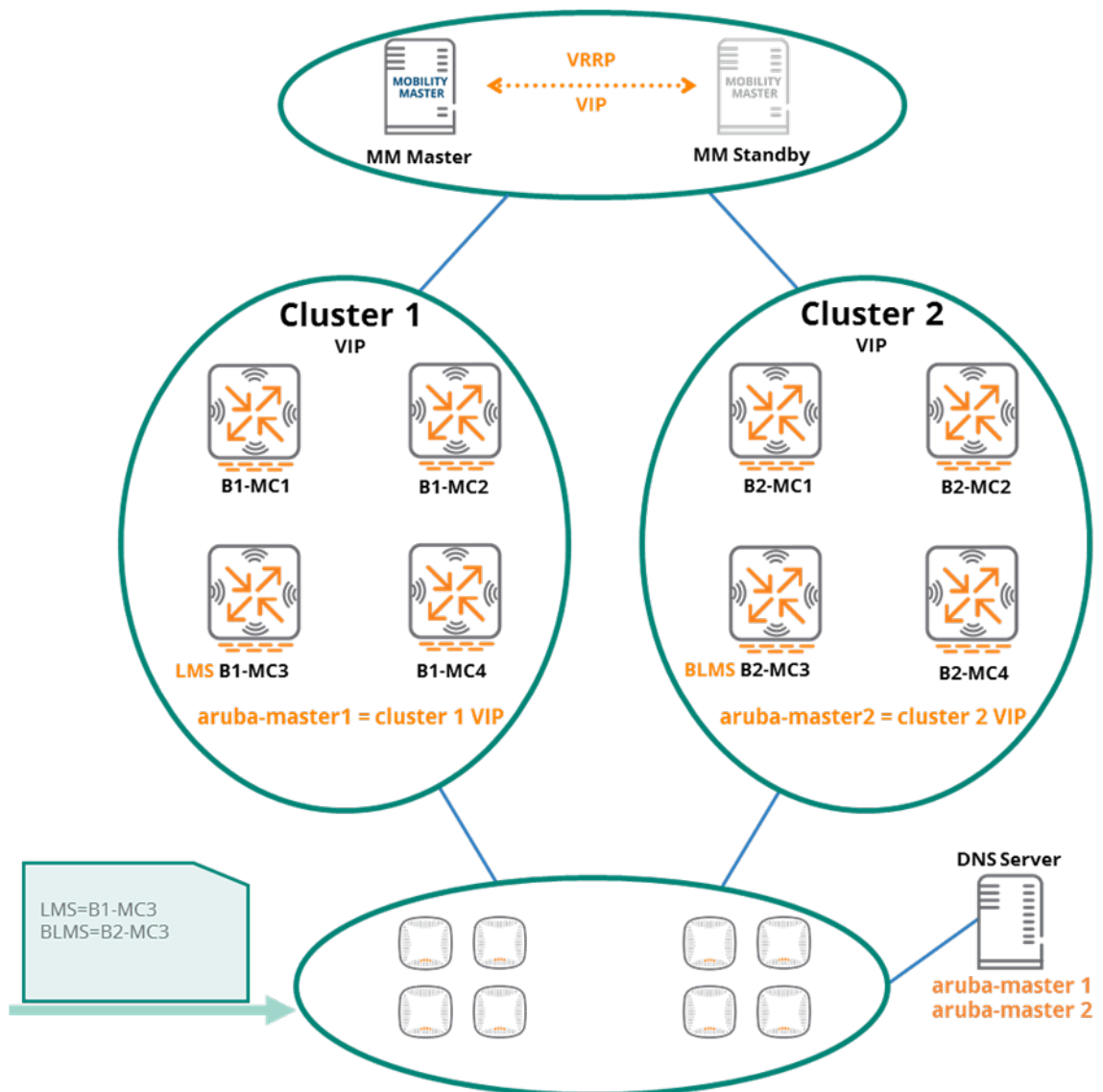


Figure 29 LMS and BLMS Architecture with Clusters

Cluster Roles

An MC can have any combination of the following four roles in a cluster aside from being the cluster leader:

1. AP Anchor Controller (AAC)
2. User Anchor Controller (UAC)
3. Standby AAC (S-AAC)
4. Standby UAC (S-UAC)

AP Anchor Controller

Anchoring is a concept that was introduced in ArubaOS 8 as part of the clustering feature set. Anchoring and clustering are designed to achieve the following objectives:

- Enhance user mobility through seamless campus roaming
- Prevent any one MC from serving a disproportionate number of APs or users
- Enable redundancy scenarios creating fault tolerance for the cluster and minimizing the impact of an MC failure

The *AP Anchor Controller (AAC)* can be thought of as the LMS for any AP that is anchored to it. Each AP receives the IP address of the LMS and once they have been terminated they will remain anchored until the cluster leader determines that they should be moved to a different cluster member. An AP is anchored to its AAC in a three step process:

1. The AP establishes active tunnels with its AAC
2. The cluster leader dynamically assigns a standby AP Anchor Controller (S-AAC) for the AP from one of the other cluster members
3. Once designated the AP established standby tunnels to the S-AAC

The AAC and S-AAC assignment process works similarly to how HA is configured however rather than having to be manually configured the process is completely dynamic. Once the AAC is designated for an AP the subsequent steps occur automatically. A visual representation of AAC assignment is displayed in the figure below:

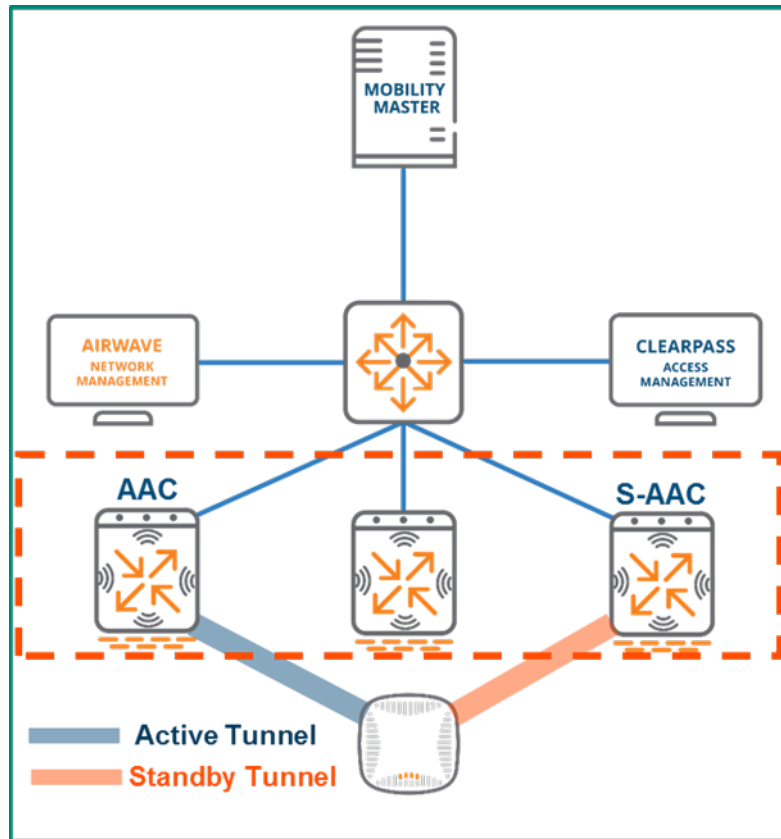


Figure 30 AAC Assignment

The AAC and S-AAC for an AP can be identified in the GUI of the MM by navigating to **Dashboard > Access Points**:

Access Points (2)		Radios (2)		Custom Columns ▾					
AP Name	Active Controller	Standby Controller	Status	Provisioned	Up time	Clients ▾	AP Mode	Model	Group
ap225-1	10.70.211.12	10.70.211.11	● up	Yes	61d:14m:9s	10	Campus	225	acme
ap325-1	10.70.211.12	10.70.211.11	● up	Yes	8d:1h:53m:36s	1	Campus	325	acme

Figure 31 AAC and S-AAC Status

While the view above indicates that the S-AAC for both APs is the same device (10.70.211.11) it should be noted that the S-AAC is assigned by the cluster leader and not all APs terminated on an AAC will have the same S-AAC. It could just as easily be a different cluster member depending on the determination made by the cluster leader based on the conditions in the cluster environment at the time of assignment.

User Anchor Controller

The concept of anchoring users to a controller using a *User Anchor Controller (UAC)* is new in ArubaOS 8 and was primarily developed to enhance the user roaming experience. When users associate to an AP, they will use the existing tunnel to their UAC if one already exists. If the AP doesn't have tunnel to their UAC established then a dynamic tunnel is created. When the client roams to a new AP, the AP they are roaming away from tears down its dynamic tunnel. User traffic is always tunneled back to their UAC regardless of which AP the client associates to as the user roams, even if that AP has a different AAC.

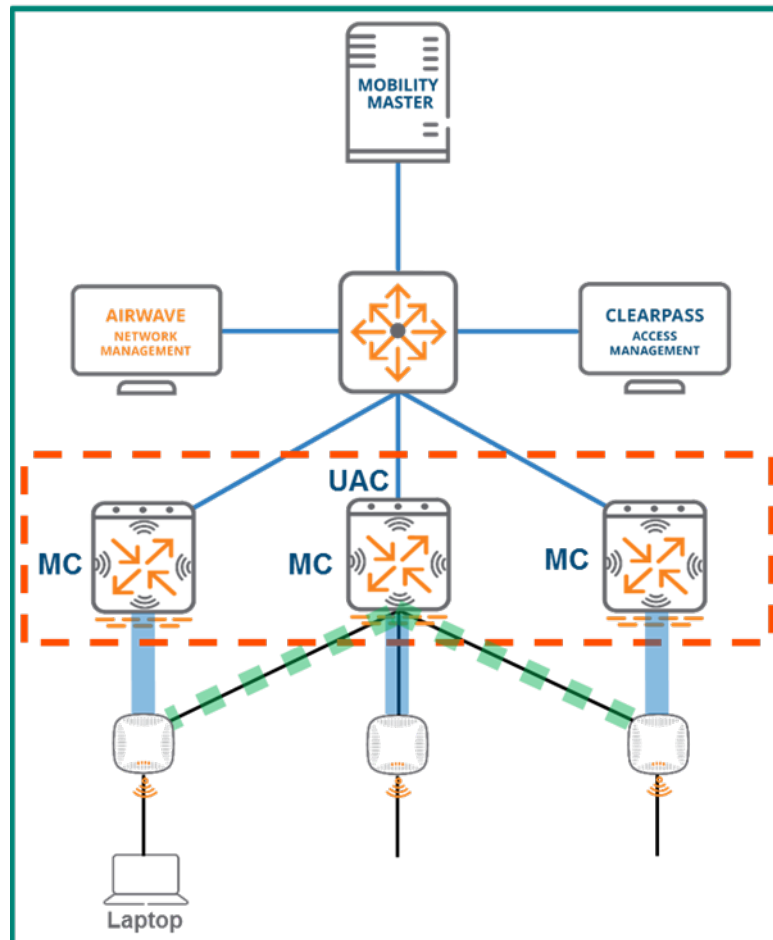


Figure 32 *Dynamic Tunnel to the Client's UAC*

In order to remain anchored, a user must first be mapped to a UAC through a hashing algorithm at the AP level. The MAC address of the client is examined and the hashing algorithm creates an index which is then compared to a mapping table. The same mapping table is pushed to all APs by the cluster leader to ensure UAC mapping consistency across the cluster. In addition, the cluster leader will dynamically select a standby UAC (S-UAC) on a per-user basis for redundancy purposes. An example of the hashing algorithm and UAC assignment process is displayed in the figure below:

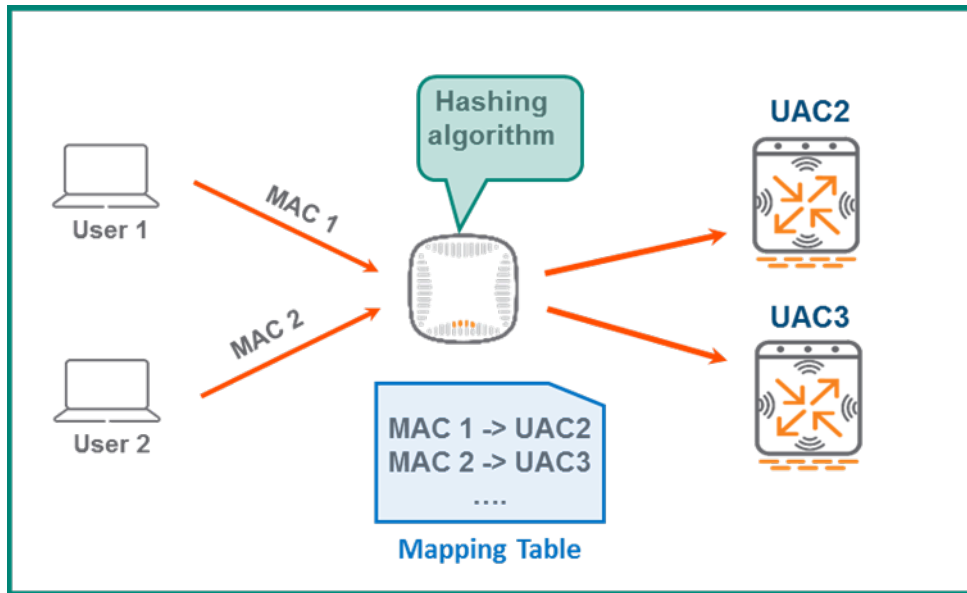


Figure 33 UAC Assignment Process

The UAC and S-UAC assignments for all associated clients can be identified in the GUI of the MM by navigating to **Dashboard > Clients**:

Client	IP Address	Health(%)	Active Controller	Standby Controller	Band	SNR (dB)	Client PHY	Role	Device
10.70.215.235	10.70.215.235	29	10.70.211.12	10.70.211.13	5 GHz	4	HT 40MHz	authenticated	Unknown
10.70.215.101	10.70.215.101	99	10.70.211.12	10.70.211.11	5 GHz	52	VHT 40MHz	authenticated	OS X
10.70.215.242	10.70.215.242	99	10.70.211.13	10.70.211.12	5 GHz	51	VHT 40MHz	authenticated	OS X
10.70.215.249	10.70.215.249	99	10.70.211.12	10.70.211.13	5 GHz	62	VHT 40MHz	authenticated	Apple
10.70.215.246	10.70.215.246	99	10.70.211.11	10.70.211.13	5 GHz	56	VHT 40MHz	authenticated	Apple
10.70.215.245	10.70.215.245	99	10.70.211.11	10.70.211.13	5 GHz	51	VHT 40MHz	authenticated	Apple
10.70.215.244	10.70.215.244	99	10.70.211.11	10.70.211.13	5 GHz	48	VHT 40MHz	authenticated	OS X
10.70.215.243	10.70.215.243	98	10.70.211.11	10.70.211.12	5 GHz	52	VHT 40MHz	authenticated	Apple
10.70.215.250	10.70.215.250	99	10.70.211.11	10.70.211.12	5 GHz	63	VHT 40MHz	authenticated	OS X
10.70.215.253	10.70.215.253	100	10.70.211.11	10.70.211.13	5 GHz	49	HT 40MHz	authenticated	Win 10

Figure 34 Client UAC and S-UAC Assignments



The Active Controller and Standby Controller columns are not included in the standard view of the Clients page in the GUI. They can be displayed by adding a customization to the page view.

Change of Authorization

Change of Authorization (CoA) is a feature which extends the capabilities of the Remote Authentication Dial-In User Service (RADIUS) protocol and is defined in RFC 5176. CoA request messages are usually sent by a RADIUS server to a network access server (NAS) device for dynamic modification of authorization attributes for an existing session. If the NAS device is able to successfully implement the requested authorization changes for the user session(s) then it will respond to the RADIUS server with a CoA acknowledgement also referred to as a CoA-ACK. Conversely, if the change is unsuccessful the NAS will respond with a CoA negative-acknowledgement or CoA-NAK.

In the context of an ArubaOS 8 cluster, unsolicited CoA requests for a user with an active session in progress are sent to that user's anchor controller. The UAC will then return an acknowledgement to the RADIUS server upon the successful implementation of the changes or a NAK in the event that the implementation was unsuccessful. However, a user's UAC may change in the course of normal cluster operations due to reasons such as an MC failure or user load-balancing events. Such a scenario would cause CoA requests to be dropped as the intended user would no longer be associated to the MC receiving the request from the RADIUS server. Aruba has implemented cluster redundancy features in order to prevent such a scenario from occurring.

Cluster CoA Support

The primary mechanism Aruba uses to provide CoA support for MC clusters in ArubaOS 8 is VRRP. In every cluster there are the same number of VRRP instances as there are nodes and each MC serves as the master of an instance. For example, a cluster with 5 MCs would have 5 instances of VRRP and 5 virtual IP addresses (VIPs). The master MC receives messages intended for the VIP of its instance while the remaining MCs in the cluster are backups for the all of other instances where they are not acting as the master. This configuration ensures that each cluster is protected by a fault-tolerant and fully redundant design.



This section describes the process of Dynamic Authorization to RADIUS as described in RFC-5176 and how RADIUS communicates with Aruba controllers in a cluster. The Change of Authorization process was selected as a representation of that communication sequence.

ArubaOS reserves VRRP instance IDs in the 220-255 range. When the master of each instance sends RADIUS requests to the RADIUS server it injects the VIP of its instance into the message as the NAS-IP by default. This ensures that CoA requests from the RADIUS server will always be forwarded correctly regardless of which MC is the acting master for the instance. I.e. the RADIUS server sends CoA requests to the current master of the VRRP instance and not to an individual station. From the perspective of the server it is sending the request to the current holder of the VIP address of the instance. The figure below depicts sample architecture that will be used for the duration of the CoA section:

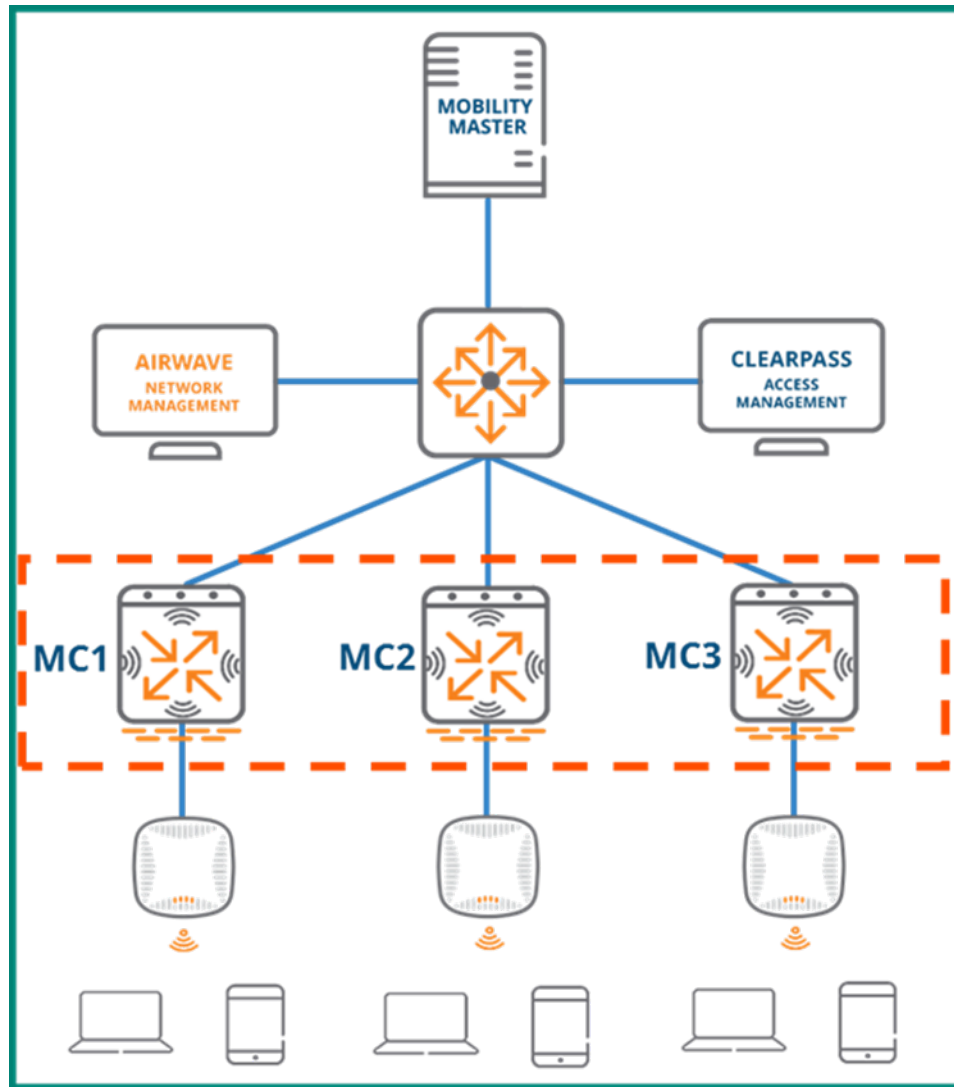


Figure 35 Sample Architecture for CoA Demonstration

This sample network consists of a three-node cluster with three instances of VRRP. The AOS-assigned VRRP ID range falls between 220 and 255 therefore the three instances in this cluster are assigned the VRRP IDs of 220, 221, and 222. The priorities for the MCs in each instance are dynamically assigned so that the master of the instance is assigned a priority of 255, the first backup is assigned a priority of 235, and the second backup is assigned a priority of 215. The table below outlines the priority assignments for each MC and each instance in the example network:

VRRP Instance	Virtual IP	MC1 Priority	MC2 Priority	MC3 Priority
ID 220	VIP1	255	235	215
ID 221	VIP2	215	255	235
ID 222	VIP3	235	215	255

Table 6 MC Priorities and VIPs for Each VRRP Instance

As demonstrated by the table, MC1 is the master of instance 220 with a priority of 255, MC2 is the first backup with a priority of 235, and MC3 is the second backup with a priority of 215. Similarly, MC2 is the master for instance 221 due to having the highest priority of 255, MC3 is the first backup with a priority of 235, and MC1 is the second backup with a priority of 215. Instance 222 follows the same pattern as instances 220 and 221.

CoA Redundancy

The failure of a cluster node is an event that can adversely impact CoA operations if the network doesn't have the appropriate level of fault tolerance. If a user's anchor controller fails, the RADIUS server will push the CoA request to their UAC as usual with the assumption that it will enforce the change and respond with an ACK. However, if a redundancy mechanism such as VRRP hasn't been implemented then the request will go unanswered and will not result in a successful change. In such a scenario the users associated with the failed node will failover to their standby UAC as usual. However, the UAC will never receive the change request from the RADIUS server since the server has no awareness of cluster operations. VRRP instances must be implemented for each node to prevent such an occurrence and maintain CoA operations in the cluster.

In the figure below MC1 is the master of instance 220 with MC2 serving as the first backup and MC3 serving as the second backup. A client associated to MC1 has been fully authenticated using 802.1X with MC3 acting as the client's standby UAC. When corresponding with ClearPass, MC1 automatically inserts VIP for instance 220 as the NAS-IP. From the perspective of ClearPass it is sending CoA requests to the current master of instance 220.

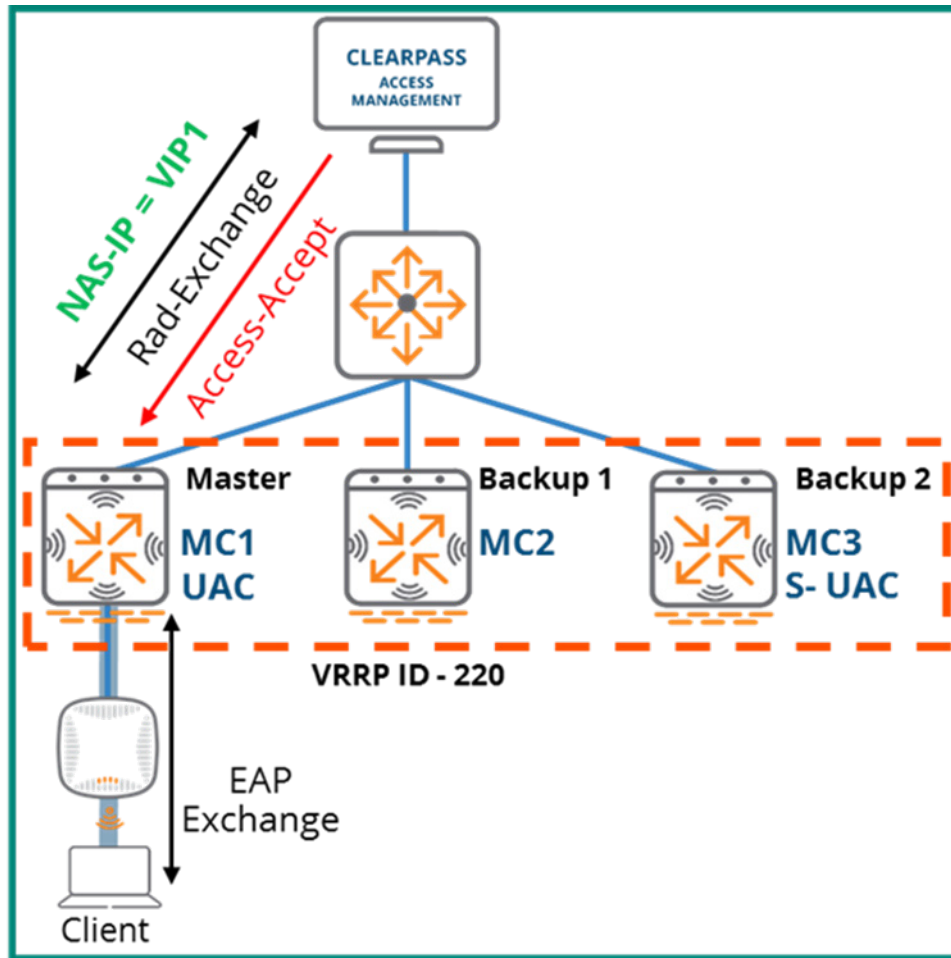


Figure 36 User Authenticates Against ClearPass

If MC1 fails while the client is in session the AP where the client is associated will failover to MC2. The client's session moves over to MC3 since it was the standby UAC. MC3 then assumes the role of UAC for the client. Since MC2 has a higher priority than MC3 in instance 220 it will assume the role of Master and take ownership of the VIP.

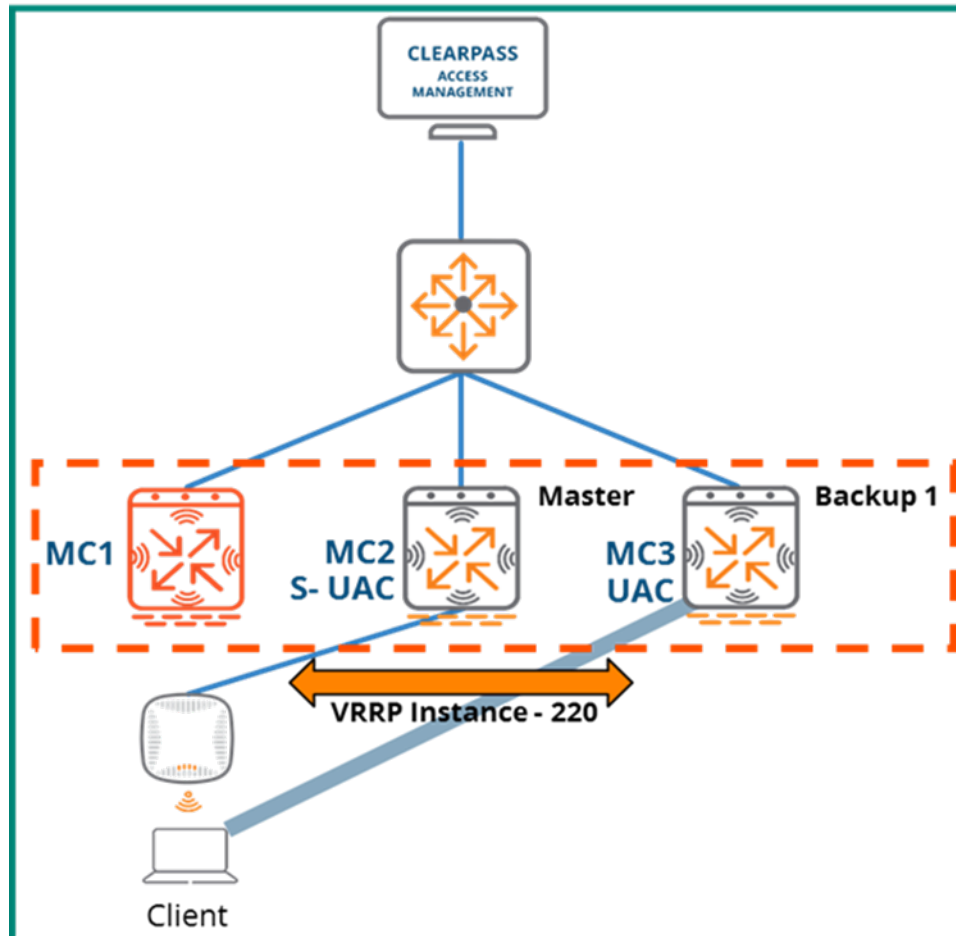


Figure 37 MC1 Failure

Any CoA requests sent by ClearPass for the client will be addressed to the VIP for instance 220. From the perspective of ClearPass, the VIP of instance 220 is the correct address for any CoA request intended for the client in the example. Since MC1 has failed, MC2 is now the Master of VRRP instance 200 and owns its virtual IP. When ClearPass sends a CoA request for the client, MC2 will receive it and then forward it to all nodes in the cluster. Since our cluster only has three nodes, in this case MC2 forwards the request to MC3.

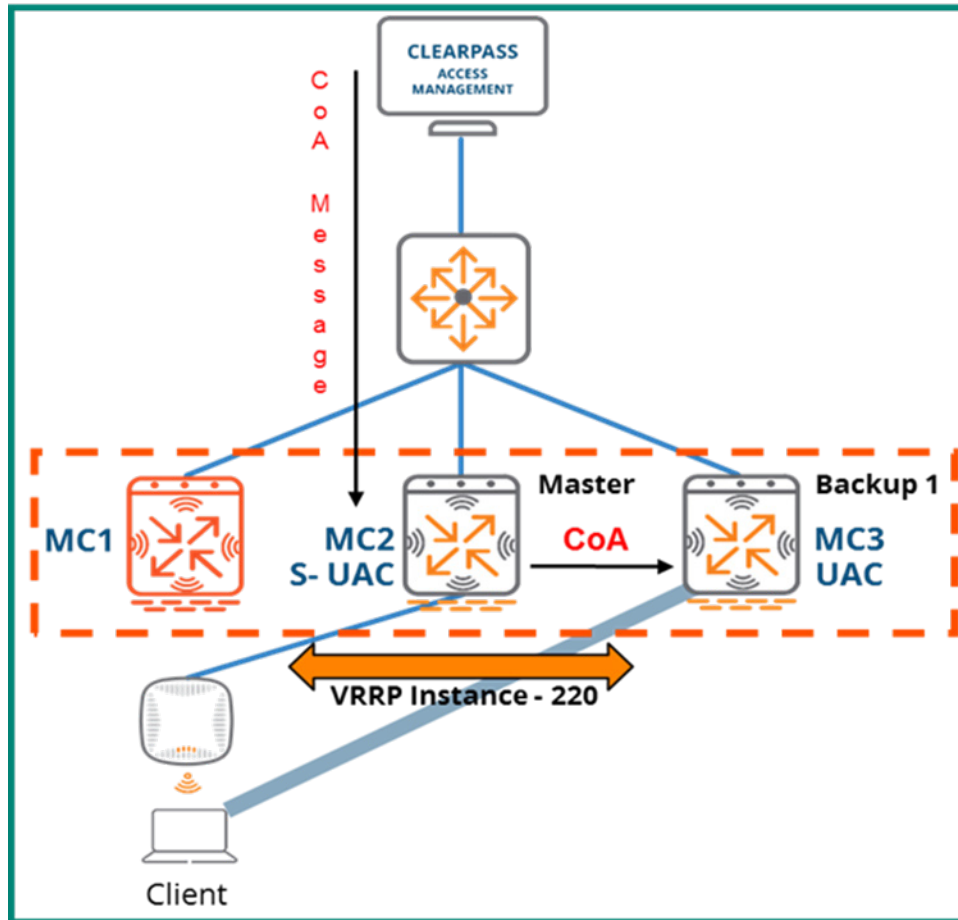


Figure 38 CoA message forwarded to MC3

After the change in the CoA request has been successfully implemented, MC3 will send a CoA-ACK back to ClearPass.

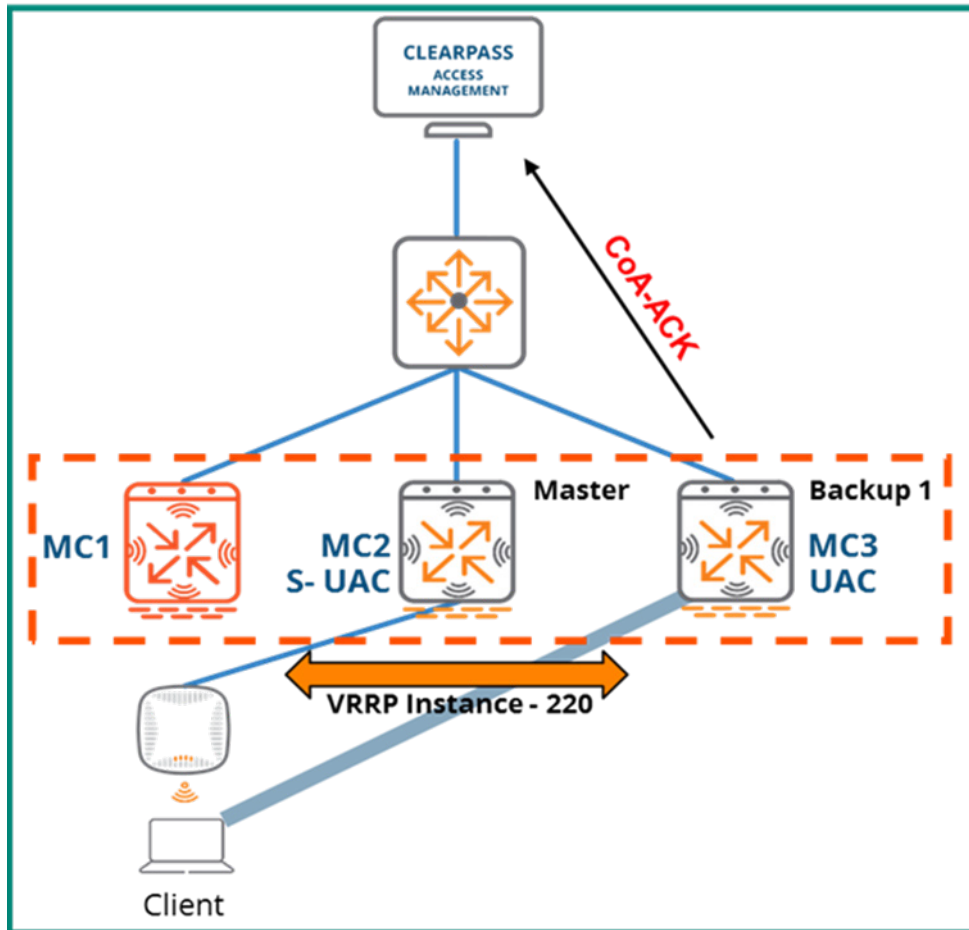


Figure 39 CoA message forwarded to MC

Network Management

Topology Description

AirWave is a network monitor and management platform that adds controllability and visibility for wired and wireless devices in any network from a single graphical interface. This kind of visibility simplifies troubleshooting, for example tracking down slow DNS, and offers deep insight into optimizing the network for specific applications such as Unified Communications and Collaboration (UCC). AMP has other features like VisualRF to help us plan spectrum and RAPIDS to protect the network from malicious attacks.

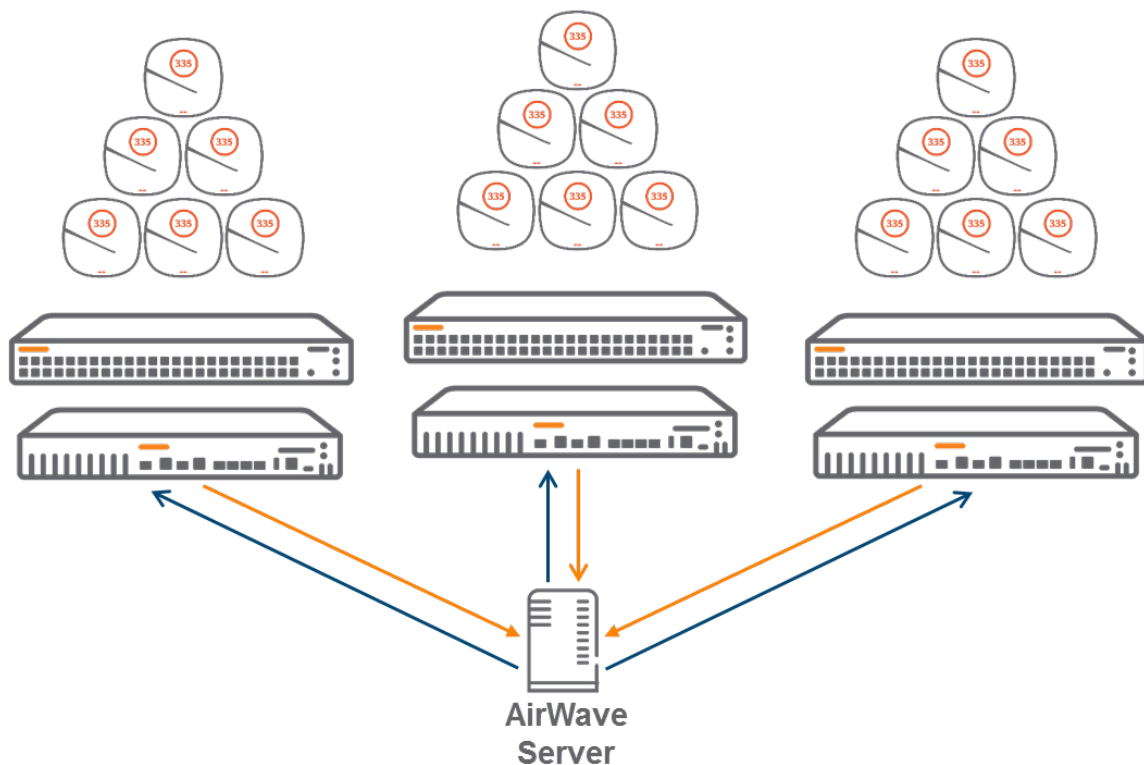


Figure 40 *AirWave Management Platform*

AMP collects data from network devices (Aruba and other brands) via protocols such as SNMP, SSH, and ICMP so administrators can view network performance either historically or in real time. Aruba controllers specifically use AMON to pass deeper information, such as AppRF, UCC, and spectrum data. HTTP Secure (HTTPS) is used for all communications when implementing Aruba Instant with AMP. Please refer to the [8.2.4 Best Practice Guide](#) for additional information on data acquisition methods.

This document assumes that an AirWave server has been installed and is reachable in the Data Center. AirWave can be deployed either virtually or as a hardware appliance. Please refer to the [8.2 Installation Guide](#) for additional details on the deployment methods for AirWave.

Monitor Only Mode

In the Mobile First Base Designs Lab Setup, AMP is only used in Monitor Only and Firmware Upgrade mode. Device management in AirWave is considered to be a specific application, outside of the scope of this VRD. In Monitor Only mode, each device is directly configured and has its static configuration imported into AirWave. AirWave can then monitor if and when a device has gone down or been changed. The Topology view of AMP shows an automatically generated overview of the network's devices with status badges to easily display the devices that are down or unhealthy. AMP uses data collected by Link Layer Discovery Protocol to build this topology.



LLDP must be enabled on the connected ports for a device to appear in the Topology. Some devices, such as controllers, have LLDP disabled by default.

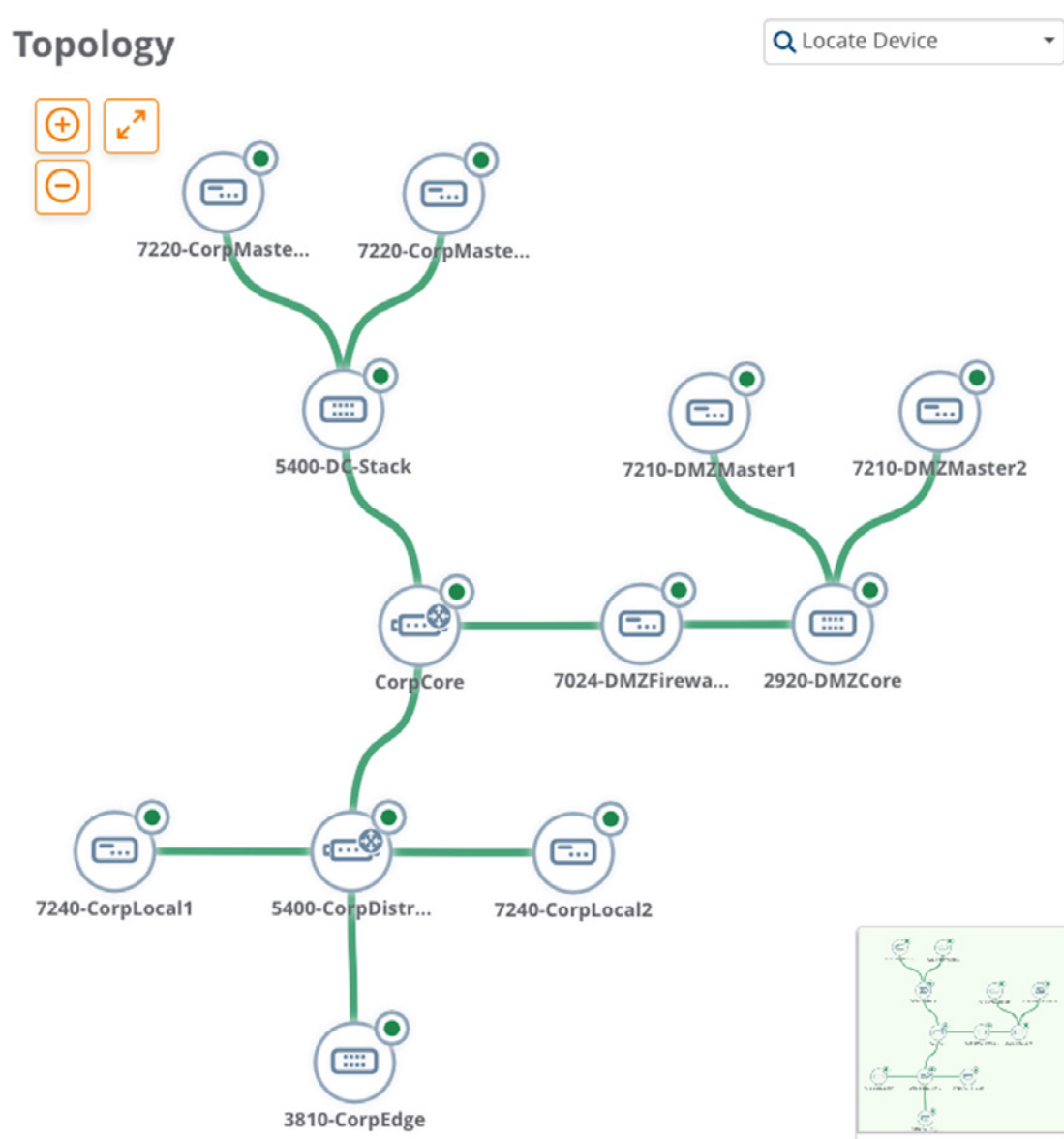


Figure 41 Topology View of AMP

Groups and Folders

AirWave device groups are generally used to organize the configurations of similar devices. AirWave will not push configuration to devices in Monitor Only Mode, however it can perform a device level configuration audit and detect mismatches.

Folders are used for organizing devices for hierarchical viewing, reporting, and permissions. The logical organization is usually done by location. This allows, for example, a certain AirWave user to only view devices in their branch by assigning folder access.

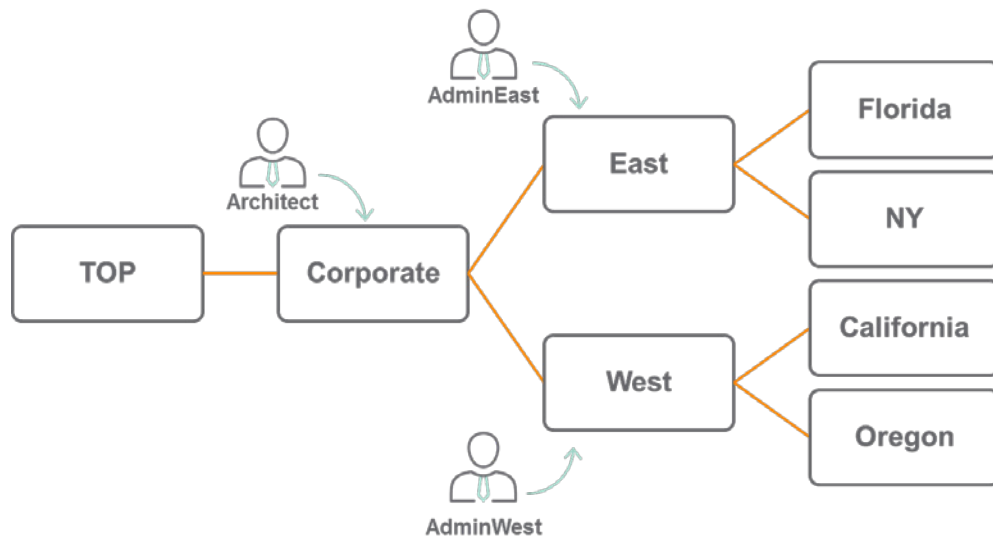


Figure 42 Sample Group and Folder Structure

In the figure above the user role AdminEast has monitor access to devices in the Florida and New York offices while AdminWest can see California and Oregon devices. The Architect role has global access to all devices in the network.

Device Discovery

In this base design, we configure devices for monitoring using SNMPv2. With polling we can manually onboard devices to AirWave. Routers, switches, and controllers require per-device SNMP community and trap-host configuration so AirWave can poll and communicate with them. Standby controllers can be discovered through the master controllers. APs are also discovered through controllers. In order to communicate client information, firewall statistics, and RF data the controllers must be configured to Enable AMON.



ZTP is another discovery option for Aruba devices using Aruba Activate or DHCP, not discussed in this VRD.



Full or partial configuration is another management scenario using Templates for Aruba devices. See Creating and Using Templates section of the AirWave User Guide.

Network Access Control

Aruba's ClearPass Network Access Control combines all the capabilities of a robust NAC solution in one centrally managed platform. The ClearPass policy server provides differentiated, context-based access control along with operational utilities designed to reduce IT overhead. With the ClearPass Policy Manager, IT can easily automate and extend authentication and authorization policies across the entire organization for wireless, wired, VPN, and guest access applications. Differentiated access capabilities are based on a variety of attributes, including user role, device, time, and location.

In addition to its integrated policy management engine and RADIUS/TACACS+ servers for AAA support ClearPass Policy is capable of multiple identity stores and databases, including those based on Microsoft Active Directory, LDAP, SQL, and Kerberos. This provides a unified policy model that ensures access controls are applied consistently across the organization.

The included standalone ClearPass Universal Profiler provides the same profiling visibility for organizations that may not be ready for full policy enforcement or for remote areas where ClearPass may not be initially deployed. Template based policy enforcement allows IT to build wired and wireless oriented policies that leverage attributes including user roles, device types, MDM/EMM data, certificate status, location, and day-of-week. Policies can easily enforce rules for employees, students, doctors, guests, executives and each of the device types that they decide to bring. The Policy Manager also includes device profiling, basic guest services, policy simulation, device registration and 25 enterprise licenses that aid in the trial of Guest, Onboard and OnGuard.



This guide was only intended to provide a general description of ClearPass in a standard ArubaOS 8 architecture. Please refer to [ClearPass documentation](#) for a more comprehensive understanding of ClearPass functionality.

Hardware and VM options for VMware ESX and Microsoft Hyper-V provide organizations with flexibility in the form factor they choose and the ability to mix and match hardware-based appliances with VM implementations without any loss of features or functionality. E.g., using VMs can reduce cost and complexity by lowering power and cooling requirements and simplifying cabling. Similarly, hardware appliances may be the best choice in larger data centers, while the VM option can be added to a server in remote offices when cost is a concern.

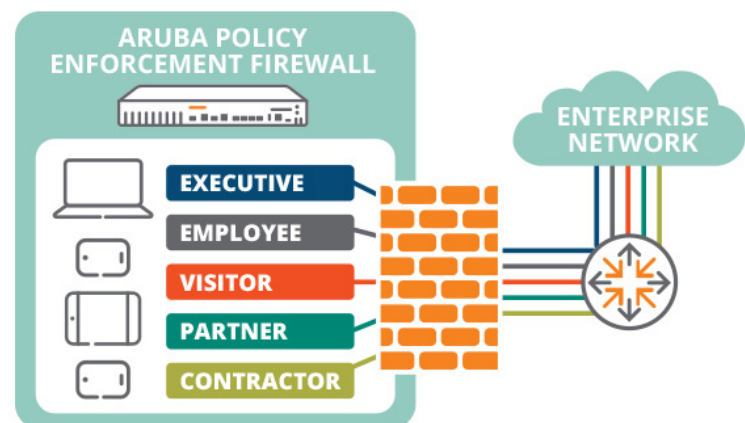


Figure 43 *ClearPass Endpoint Profiler*

Lab Design and Addressing

Service Set Identifiers

This section outlines details pertaining to the three example SSIDs that are configured for this Mobile First Base Design Lab Setup:

- byod_employee
- psk_corp
- guest

A prefix of “TME-MobileFirst-” has been added to each SSID to facilitate identification in a high-density testing environment.

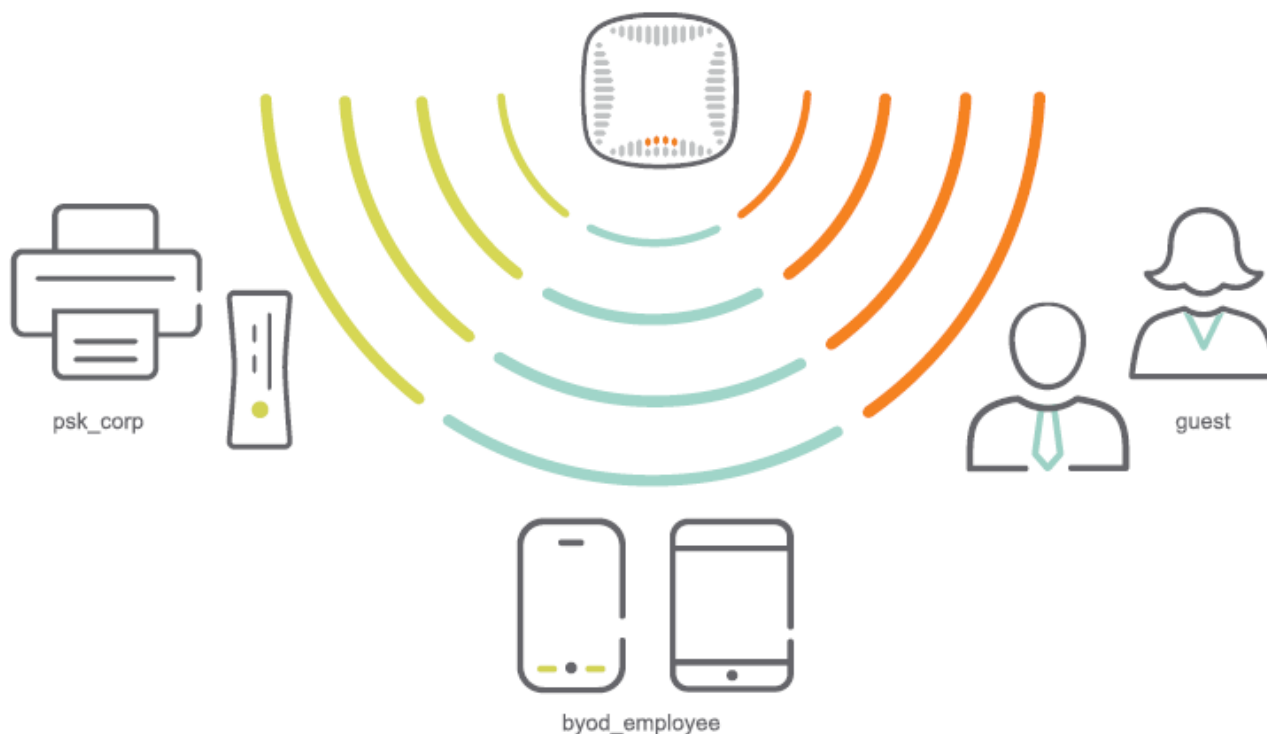


Figure 44 Configured SSIDs for the Test Network

TME-MobileFirst-byod_employee

This SSID is for employee clients to connect their mobile phones, laptops, and other personal devices to the corporate network. Traffic on this SSID is held in VLAN 225 and is handled by the MCs. CP-Corp is configured as our RADIUS server and to host an Onboarding page.

The bring your own device (BYOD) deployment is a combination of 802.1X authentication and onboarding portal to enforce the use of Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), certificate-based authentication.

ClearPass Onboard relieves the burden of deploying certificates for every user. The *TME-MobileFirst-byod_employee* wireless network allows a first-time corporate client to connect using Extensible Authentication Protocol-Protected (EAP-PEAP) with a limited access user role called *onboard*. During the onboarding process clients are redirected to a captive portal where they are prompted to install a certificate and network profile. Post installation the client is able to authenticate with EAP-TLS. The client then deauthenticates and then reconnects with the new network profile using EAP-TLS. Upon recognizing clients connecting to the *TME-MobileFirst-byod_employee* SSID using EAP-TLS ClearPass automatically profiles the user with the *TME-MobileFirst-byod_employee* user role. This role then grants the user full network access.

TME-MobileFirst-psk_corp

This SSID is for clients that do not support 802.1X authentication, such as printers, scanners, or other application-specific machines. Traffic on this SSID is held in VLAN 226 and is handled by the MCs, configured for Wi-Fi Protected Access 2-Pre-Shared Key (WPA2-PSK) authentication. The *TME-MobileFirst-psk_corp* SSID could also potentially be used to accommodate IoT (Internet of Things) devices.

TME-MobileFirst-Guest

This SSID is for guests visiting the physical campus to connect their mobile phones, laptops, and so on, to access the Internet. Guest clients do not need access to the corporate network and are therefore handled in the DMZ by DMZ-MCs and ClearPass-DMZ, the separate ClearPass server. From the DMZ, guest clients can reach the internet by Network Address Translation (NAT) inside the firewall. Using this SSID, guests can reach the Internet after a L3 captive portal self-registration with Media Access Control (MAC) caching.

VLAN 999 holds the traffic on this SSID. VLAN 999 belongs in the DMZ, but is extended through L2 generic routing encapsulation (GRE) tunnels to the LCs, where all of the APs terminate.

Guest Access

The Guest SSID used in the Mobile First Base Designs Lab Setup supports a guest captive portal served from the ClearPass server. The user is then taken through a self-registration process, followed by caching the MAC address of the end client. The MAC caching enables seamlessly joining the guest network for the duration the MAC is cached in the ClearPass “known device” repository until the timeout. Once the MAC cache for an end client expires, the client is redirected to self-registration again.

The following steps with diagrams explain the flow.

1. A new guest fails MAC authentication for the first time, and is redirected to the captive portal login page for guest registration.

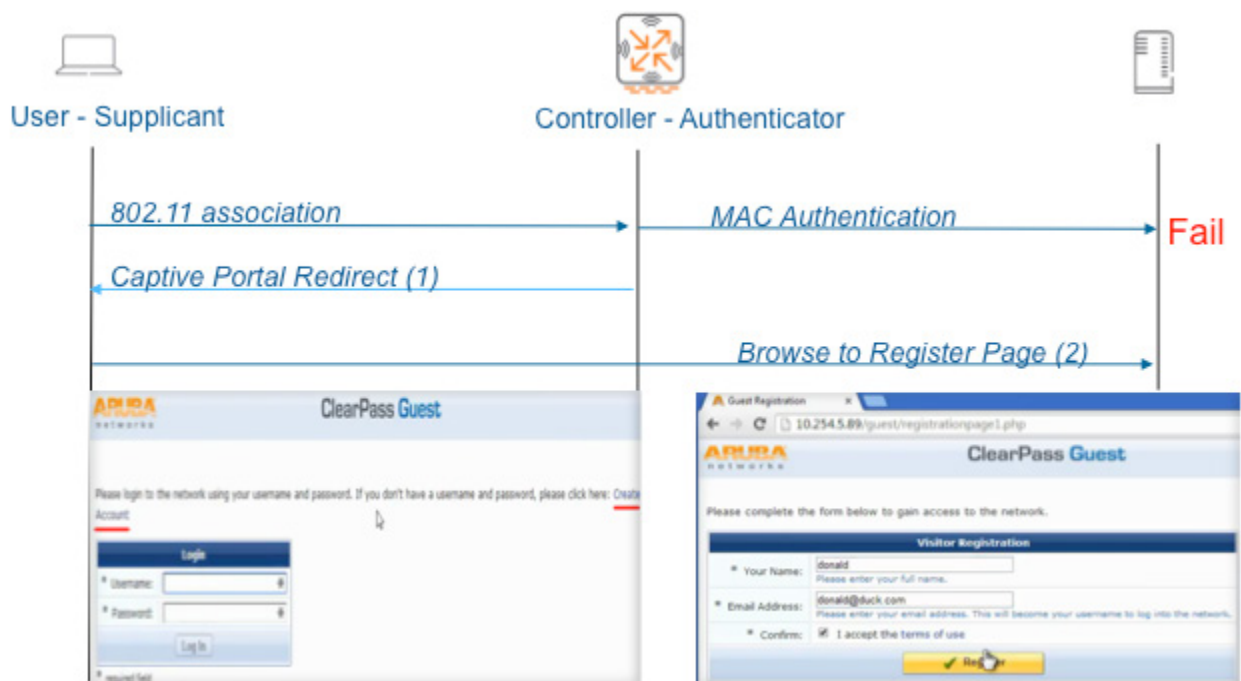
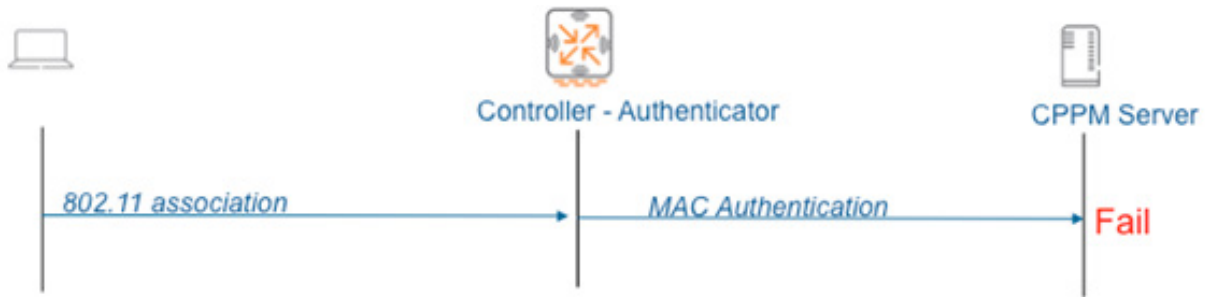


Figure 45 Guest Registration

2. The guest user's MAC address is added into the Endpoints Repository with an Unknown status in the ClearPass server.



Configuration > Identity > Endpoints

Endpoints

Filter: MACAddress contains f294 Go Clear Filter

#	MAC Address	Hostname	Category	OS Family	Status
1.	00216a64f294	nbhave-x200	Computer	Windows	Unknown

Showing 1-1 of 1

Figure 46 Endpoints Unknown Status

- Guest user finishes registration, gets a valid username and password, and the user entry is added into the guest user repository.

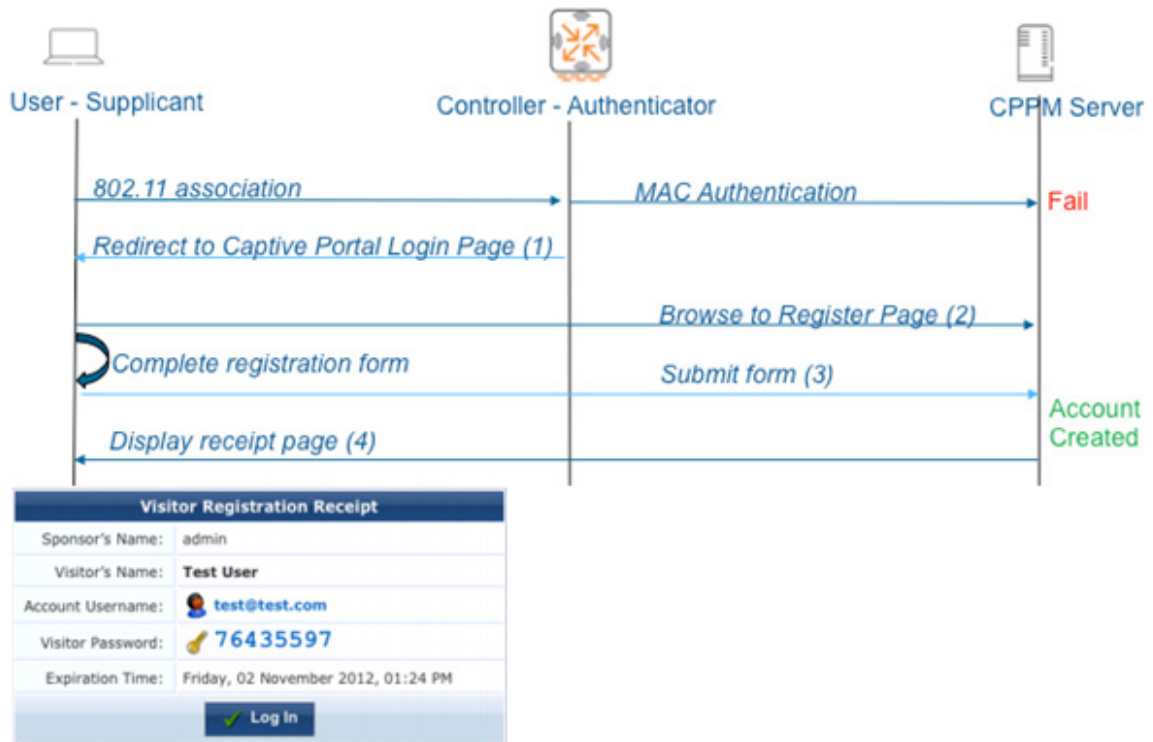
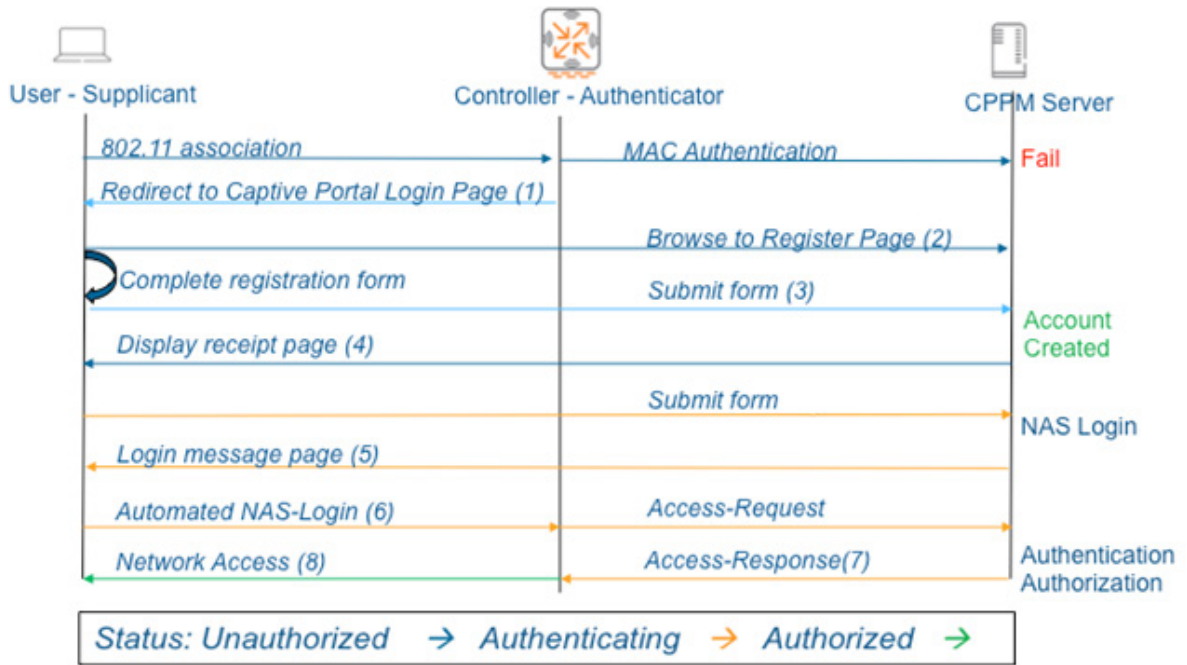


Figure 47 Guest User Repository

- Guest user passes captive portal authentication and user MAC address is added as a 'Known' endpoint in the ClearPass device repository.



Configuration » Identity » Endpoints

Endpoints

Filter: MAC Address contains f294 Go Clear Filter

#	MAC Address	Hostname	Category	OS Family	Status
1.	00216a64f294	nbhave-x200	Computer	Windows	Known

Figure 48 MAC Address Known Endpoint

- For example, say the MAC caching timeout on the ClearPass server is set to 8 hours. If the end client were to drop off the guest network and connect back within 8 hours, in the next 1 hour, MAC authentication succeeds and the user is granted access. There is no need for captive portal authentication again.

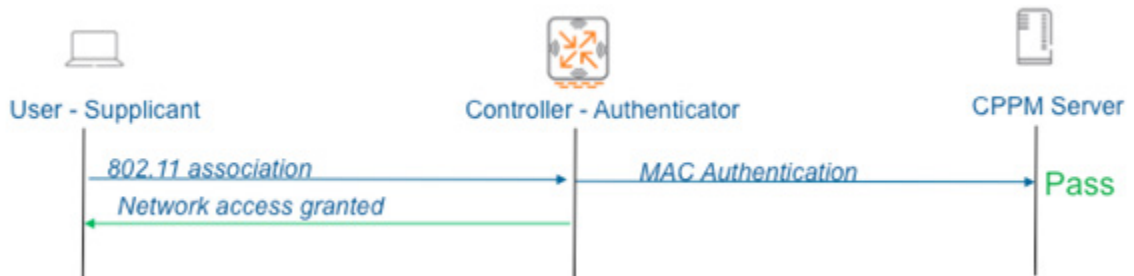


Figure 49 Network Access Granted

- Once the MAC cache on ClearPass expires after 8 hours, and guest returns after the MAC cache timeout, MAC authentication once again fails and the user is redirected to the captive portal self-registration page once again, for captive portal authentication.

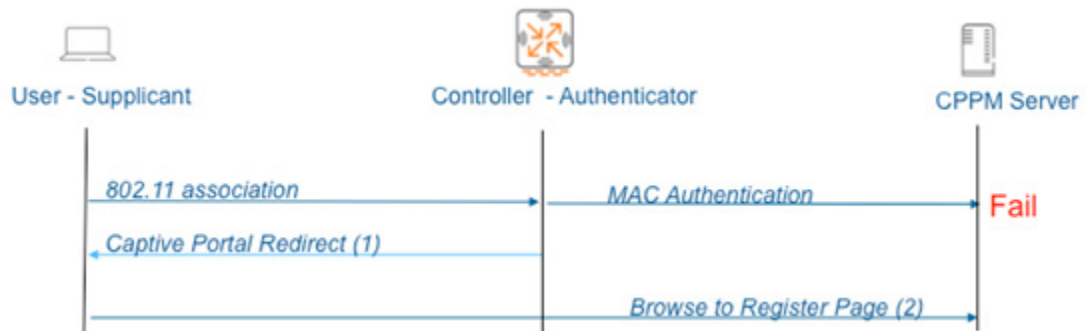


Figure 50 Captive Portal Redirect to Registration Page

802.1X Authentication

802.1X authentication is widely used in enterprises as the primary mode of authenticating wireless and wired clients. This section touches upon the PEAP and EAP-TLS packet flows. The RADIUS server in these examples is a ClearPass server.

The packet flows assume that the ClearPass server is configured to connect to a user database in the form of Active Directory in case of PEAP authentication, and certificates are installed on the ClearPass and end clients for EAP-TLS authentication.

EAP-PEAP Authentication

EAP-PEAP authentication is usually username and password-based.

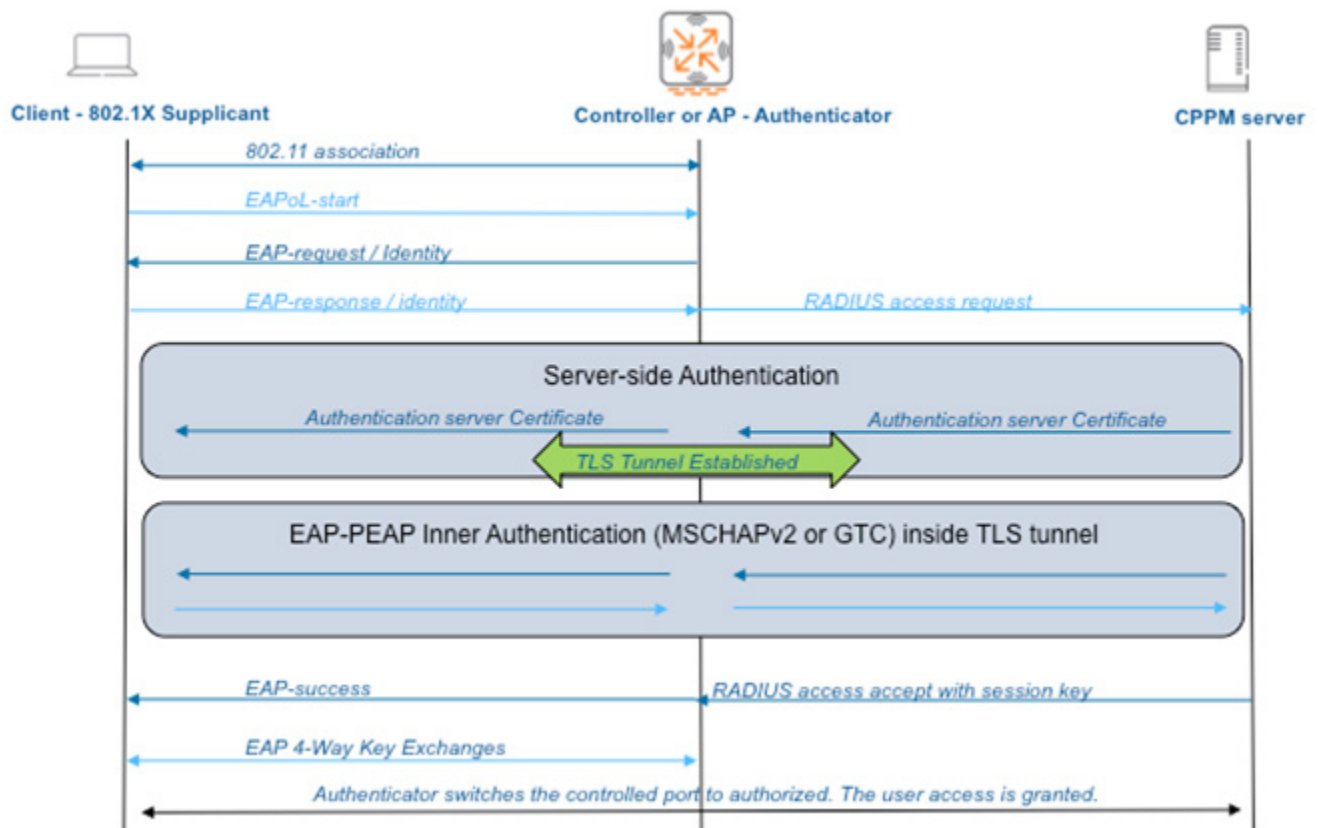


Figure 51 EAP-PEAP Authentication Packet Flow

EAP-TLS Authentication

EAP-TLS authentication is certificate-based authentication. This type of authentication involves installing a certificate on each end client and the RADIUS server. Certificates are used to identify the client to the server and vice versa.

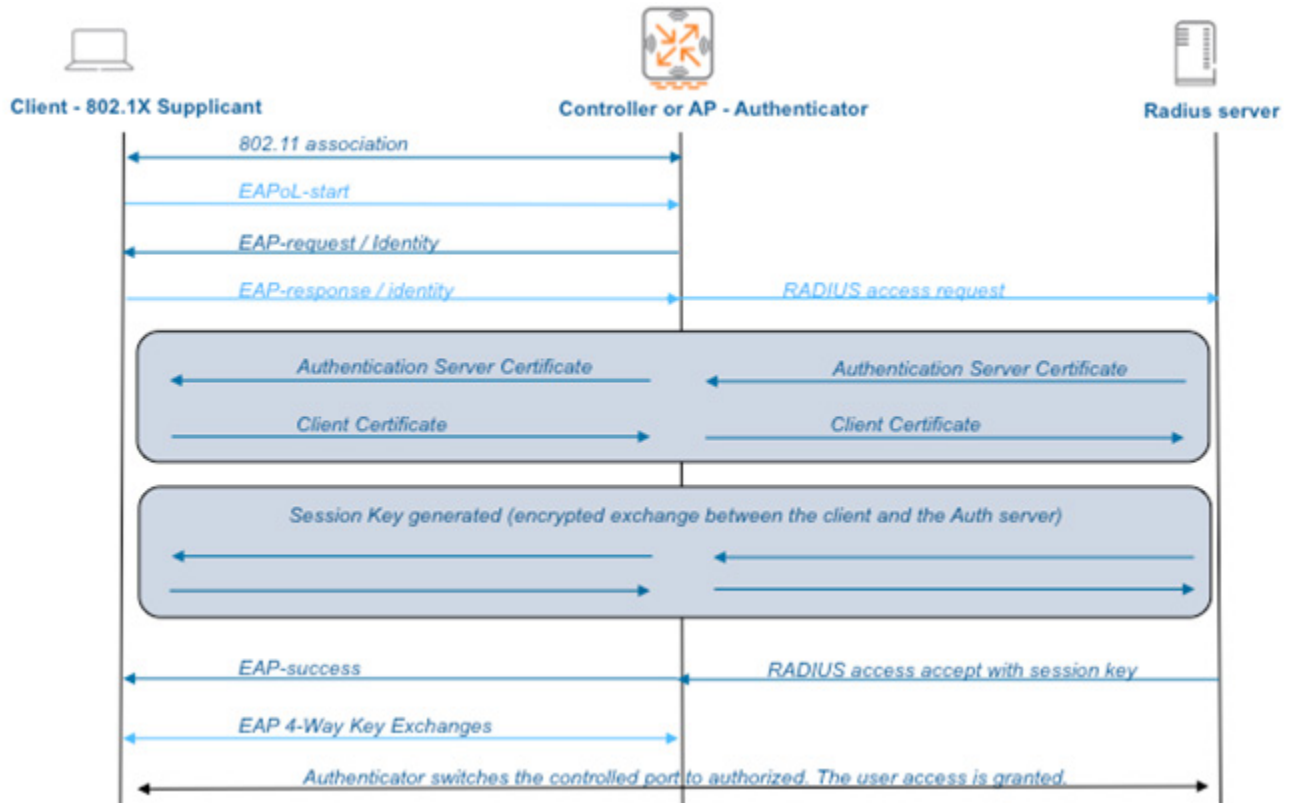


Figure 52 EAP-TLS Authentication Packet Flow

BYOD SSID Configuration

EAP-PEAP/MSCHAPv2 with Active Directory (AD), although one of the most popular and widely used methods by enterprises for authentication, is known to have some inherent security drawbacks, that make it prone to Denial of Service (DoS) and Man in the Middle attacks. The BYOD flow explained here is one of the most common and widely used by our customers today, that uses a single SSID to achieve both on-boarding and secure access to employees.

The following onboarding flow involves using EAP-PEAP/MSCHAPv2 with AD for initial connection to the network. This may be deemed insecure by certain customers. There are alternative BYOD methods/flows that can be recommended to such customers, which are not covered in this version of the Mobile First Base Designs Lab Setup and will be addressed in a future release of this document.

The BYOD SSID used in this Mobile First Base Designs Lab Setup is an important network, which will be used for on-boarding employee devices on the corporate network. The on-boarding process gives the corporate security administrators an opportunity to provision employee devices that are not corporate issued.

The provisioning process usually entails installing certificates on the end client devices and steering the client to use EAP-TLS, which is a more secure way of connecting to the network. The provisioning process may also involve running a security check on the end client device, not covered in this flow.

To support on-boarding/BYOD, it is not required to have a separate BYOD SSID. This also helps in reducing the number of SSIDs being advertised. A single SSID can be configured as EAP-PEAP and EAP-TLS to support onboarding. During on-boarding client devices are connected using EAP-PEAP, at the end of on-boarding the client device is reassociated using EAP-TLS.



As EAP-PEAP and EAP-TLS flows have already been explained in the preceding sections this section will only outline web-login redirect and device provisioning flows

1. **EAP-PEAP** - All employees are assumed to be assigned a domain login - username/password. Employee connects to the BYOD SSID using the username and password assigned to them. At this stage the employee's personal device connect to the corporate network using EAP-PEAP authentication (note that the EAP-PEAP packet flow is the same as explained in the previous section).
2. **On-Boarding** - The user device is still placed in a very restrictive role, just like a guest is placed in a restrictive role and can access only a captive portal.
3. **On-Boarding** - When the user attempts to access a Hypertext Transfer Protocol (HTTP) location, the device that just authenticated using EAP-PEAP is redirected to another 'web-login' page. The user enters the same username and password on that web-login page, upon which the user is redirected to the *provisioning page*.
4. **On-Boarding** - The provisioning page usually involves running a provisioning routine. This includes installing a certificate on the client device, and reconfiguring the SSID profile on the client device to use the EAP-TLS certificate based authentication as opposed to the EAP-PEAP authentication that the employee used earlier.

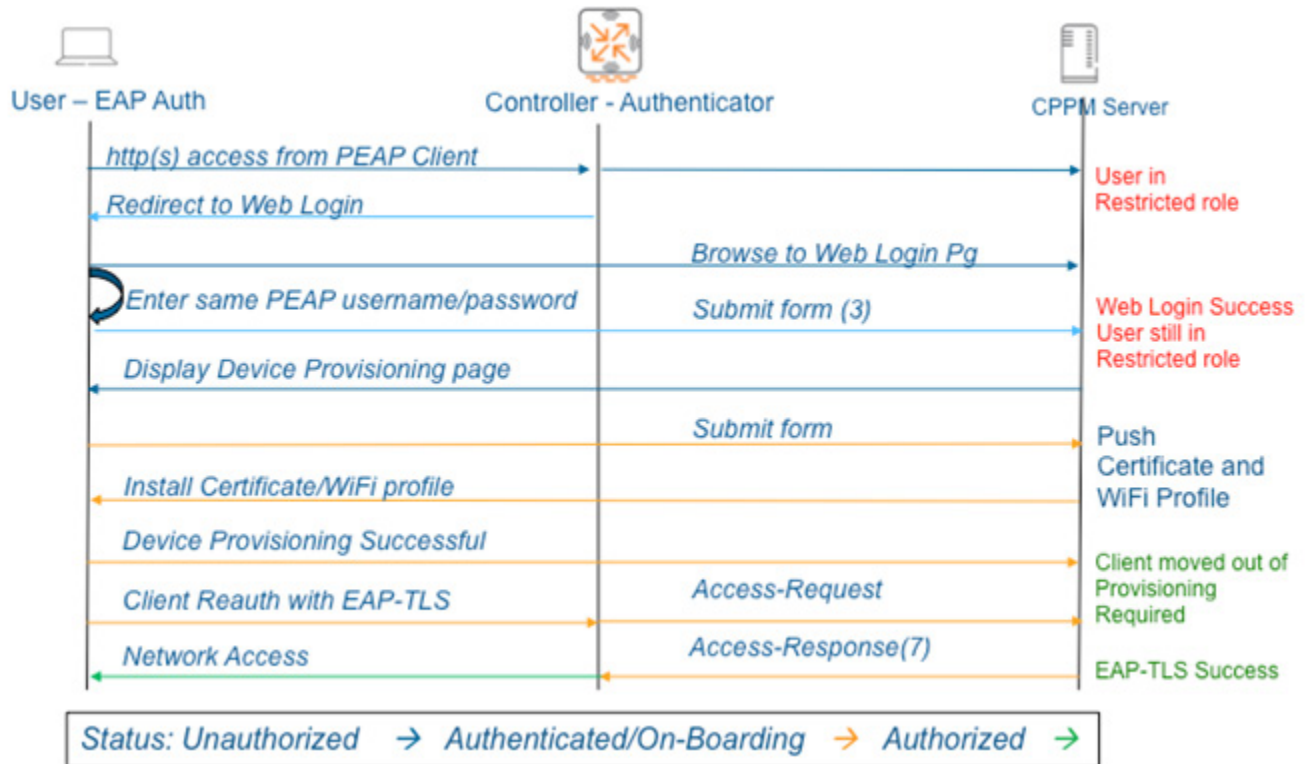


Figure 53 On-Boarding Flow

- Client Re-authentication EAP-TLS** - Once the device is provisioned, the device's connection is bounced (or has to be bounced manually) to reconnect to the 'same' SSID, but this time using EAP-TLS certificate-based authentication. After this EAP-TLS authentication, the client device is in an unrestricted role, like an employee. Thus, the employee device is now on-boarded (note that the EAP-TLS packet flow is the same as explained in the previous section).

Lab Setup

VLANS and Subnets

The table below describes the assignments for VLANs and subnets within the Aruba campus lab network:

Purpose	VLAN	Subnet
Network Services	3	10.127.3.0/24
Servers	89	10.127.89.0/24
Mobility Controller Management	90	10.127.90.0/24
Switch Management	91	10.127.91.0/24
Access Point Management	92	10.127.92.0/24
DMZ Management	93	10.127.93.0/24
byod_employee SSID Clients	95	10.127.95.0/24
psk_corp SSID Clients	96	10.127.96.0/24
guest SSID Clients	999	192.168.1.0/24

Table 7 Lab VLANs and Subnets

Data Center Components and Addressing

Host	Description	VLAN	IP
WIN2016-Corp	Server for AD, DNS, and DHCP	3	10.127.3.11
MM-VIP	Mobility Master Virtual IP (VRRP-VIP)	89	10.127.89.10
MM-01	Mobility Master Active	89	10.127.89.11
MM-02	Mobility Master Standby	89	10.127.89.12
Airwave-Corp	AirWave Network Monitoring	89	10.127.89.20
CP-Corp	Campus ClearPass Server	89	10.127.89.30
MC-Cluster-VIP	Mobility Controller Cluster Virtual IP	90	10.127.90.10
MC-Cluster-CoA-01	MC Cluster Change of Authority (CoA) VIP 1 - VRRP 220	90	10.127.90.21
MC-Cluster-CoA-02	MC Cluster CoA VIP 2 - VRRP 221	90	10.127.90.22
MC-Cluster-CoA-03	MC Cluster CoA VIP 3 - VRRP 222	90	10.127.90.23
MC-Cluster-CoA-04	MC Cluster CoA VIP 4 - VRRP 223	90	10.127.90.24

MC-01	Mobility Controller - Cluster Node 1	90	10.127.90.11
	byod_employee Captive Portal Requirement	95	10.127.95.11
MC-02	Mobility controller Cluster Node 2	90	10.127.90.12
	byod_employee Captive Portal Requirement	95	10.127.95.12
MC-03	Mobility Controller - Cluster Node 3	90	10.127.90.13
	byod_employee Captive Portal Requirement	95	10.127.95.13
MC-04	Mobility Controller - Cluster Node 4	90	10.127.90.14
	byod_employee Captive Portal Requirement	95	10.127.95.14

Table 8 Data Center Components and Addressing

Wired LAN Components and Addressing

Host	Description	VLAN	IP
SW-TOR-LAB	L3 top-of-the-rack Switch		
	*Interconnect to Aruba-IT	88	10.127.88.2
	*Interconnect to SW-Core	98	10.127.98.1
	*Interconnect to FW-DMZ	99	10.127.99.1
SW-Core	Core Campus Switch - Pair of HPE 5400R in VSF		
	Default Router for Servers	89	10.127.89.1
	Default Router for Mobility Controllers	90	10.127.90.1
	Default Router for Switches	91	10.127.91.1
	Default Router for Access Points	92	10.127.92.1
	Default Router for 'Byod_Employee' Clients	95	10.127.95.1
	Default Router for 'Psk_Corp' Clients	96	10.127.96.1
	*Interconnect to SW-TOR-LAB	98	10.127.98.2
SW-Access-01	Access Switch - HPE 3810 PoE+	91	10.127.91.101
AP-2XX	Various Access Points For WLAN Testing	92	10.127.92.X
AP-3XX	Various Access Points For WLAN Testing	92	10.127.92.X

Table 9 Wired LAN Components and Addressing

Demilitarized Zone

Host	Description	VLAN	IP
WIN2016-DMZ	Server for DNS and DHCP	93	10.127.93.5
MC-DMZ-VIP	DMZ Mobility Controller Virtual IP	93	10.127.93.10
MC-DMZ-01	DMZ Standalone Mobility Controller 1	93	10.127.93.11
	guest SSID Captive Portal Requirement	999	192.168.1.11
MC-DMZ-02	DMZ Standalone Mobility Controller 2	93	10.127.93.12
	guest SSID Captive Portal Requirement	999	192.168.1.12
SW-AGG-DMZ	DMZ Aggregation Switch	93	10.127.93.2
	Guest SSID DHCP Server	999	192.168.1.2
CP-DMZ	DMZ ClearPass Server	93	10.127.93.30
FW-DMZ	DMZ-Internet Edge Firewall	93	10.127.93.1
	Default Router for Guest SSID Clients	999	192.168.1.1
	*Interconnect to SW-TOR-LAB	99	10.127.99.2

Table 10 DMZ Components and Addressing

Configuration

When building an ArubaOS 8 architecture certain steps must be followed in order to ensure proper functionality. The wired network needs to be built first because the ArubaOS 8 controller-based WLAN is an overlay and requires it to function. The network Core is configured first followed by the Aggregation and Access layer devices. Once the wired network has been properly configured the wireless components can be layered on top of it. The wireless network is established from Data center level down to APs at the Access layer. The DMZ equipment is configured last, again from top to bottom.

Upon completion of this chapter, the devices will be pingable and their Web user interfaces (WebUI) will be functional. If replicating this configuration in a production or even in a test lab environment it is important to keep the following points concerning ArubaOS switch configuration in mind:

- The word “trunk” refers to a named group of physical links (or LAG), but it does not refer to a “VLAN trunk”
- A VLAN added to a “VLAN trunk” is referred to as “tagged”. An “access” port on an ArubaOS switch is “untagged”
- On an ArubaOS switch ports are added to a VLAN, whereas on an ArubaOS WLAN Controller VLANs are added to a port
- Ports on a modular ArubaOS switches are labeled using the following convention: Chassis number/module letter/port number if they are configured as part of VSF. E.g., port 20 on module B installed on chassis 1 would be represented in the following manner: 1/B/20

SW-TOR-LAB

The SW-TOR-LAB switch serves as the uplink for the Mobile First Base Designs Lab for ArubaOS 8 VRD test lab network and connects the lab network to Aruba's corporate IT network. It also serves as a layer 3 hop between the corporate zone and the demilitarized zone.

```
Aruba-2930F-8G-PoEP-2SFPP# configure terminal
```

Enter configuration mode

```
Aruba-2930F-8G-PoEP-2SFPP(config)# hostname SW-TOR-LAB
```

Change the hostname

```
SW-TOR-LAB(config)# trunk 3-4 trk2 lacp
```

```
SW-TOR-LAB(config)# trunk 5-6 trk3 lacp
```

Add ports into LAGs

```
SW-TOR-LAB(config)# vlan 88
```

```
SW-TOR-LAB(vlan-88)# name 88-Interconnect_TOR-to-IT
```

```
SW-TOR-LAB(vlan-88)# ip address 10.127.88.2 255.255.255.0
```

```
SW-TOR-LAB(vlan-88)# exit
```

Internal configuration, not necessary outside of the Aruba test lab

```
SW-TOR-LAB(config)# vlan 89
```

```
SW-TOR-LAB(vlan-89)# name 89-Servers
```

```
SW-TOR-LAB(vlan-89)# tagged Trk2
```

```
SW-TOR-LAB(vlan-89)# exit
```

Add VLAN 89 for Servers tagged on Trk2

```
SW-TOR-LAB(config)# vlan 90
```

```
SW-TOR-LAB(vlan-90)# name 90-MobilityControllerMgmt
```

```
SW-TOR-LAB(vlan-90)# exit
```

Add VLAN 90 for controller management

```
SW-TOR-LAB(config)# vlan 91
```

```
SW-TOR-LAB(vlan-91)# name 91-SwitchMgmt
```

```
SW-TOR-LAB(vlan-91)# exit
```

Add VLAN 91 for switch management

```
SW-TOR-LAB(config)# vlan 92
```

```
SW-TOR-LAB(vlan-92)# name 92-AccessPoint
```

```
SW-TOR-LAB(vlan-92)# exit
```

Add VLAN 92 for APs

```
SW-TOR-LAB(config)# vlan 93
```

```
SW-TOR-LAB(vlan-93)# name 93-DMZ
```

```
SW-TOR-LAB(vlan-93)# exit
```

Add VLAN 93 for the DMZ


```
SW-TOR-LAB(config)# vlan 95
SW-TOR-LAB(vlan-95)# name 95-ByodClients
SW-TOR-LAB(vlan-95)# exit
```

Add VLAN 95 for BYOD clients

```
SW-TOR-LAB(config)# vlan 96
SW-TOR-LAB(vlan-96)# name 96-PskClients
SW-TOR-LAB(vlan-96)# exit
```

Add VLAN 96 for PSK clients

```
SW-TOR-LAB(config)# vlan 98
SW-TOR-LAB(vlan-98)# name 98-Interconnect_TOR-to-Core
SW-TOR-LAB(vlan-98)# untagged Trk2
SW-TOR-LAB(vlan-98)# ip address 10.127.98.1 255.255.255.0
SW-TOR-LAB(vlan-98)# exit
```

Add VLAN 98 to connect the TOR switch to the network Core untagged on Trk2

```
SW-TOR-LAB(config)# vlan 99
SW-TOR-LAB(vlan-99)# name 99-Interconnect_TOR-to-DMZ-FW
SW-TOR-LAB(vlan-99)# untagged Trk3
SW-TOR-LAB(vlan-99)# ip address 10.127.99.1 255.255.255.0
SW-TOR-LAB(vlan-99)# exit
```

Add VLAN 99 to connect the TOR switch to the DMZ untagged on Trk3

```
SW-TOR-LAB(config)# interface 1
SW-TOR-LAB(eth-1)# tagged vlan 88-99
SW-TOR-LAB(eth-1)# exit
```

Specify all VLANs tagged on Interface 1

```
SW-TOR-LAB(config)# interface 2
SW-TOR-LAB(eth-2)# disable
SW-TOR-LAB(eth-2)# exit
```

Disable Interface 2

```
SW-TOR-LAB(config)# ip route 0.0.0.0/0 10.127.88.1
```

Default route to the internal Aruba network

```
SW-TOR-LAB(config)# ip route 10.127.89.0/24 10.127.98.2
```

Route from Servers to internal Aruba network

```
SW-TOR-LAB(config)# ip route 10.127.90.0/24 10.127.98.2
```

Route from Mobility Controllers to internal Aruba network

```
SW-TOR-LAB(config)# ip route 10.127.91.0/24 10.127.98.2
```

Route from Switch
Management to internal
Aruba network

```
SW-TOR-LAB(config)# ip route 10.127.92.0/24 10.127.98.2
```

Route from APs to internal
Aruba network

```
SW-TOR-LAB(config)# ip route 10.127.93.0/24 10.127.99.2
```

Route from DMZ to the
internal Aruba network

```
SW-TOR-LAB(config)# ip route 10.127.95.0/24 10.127.98.2
```

Route from the BYOD SSID
to the internal Aruba
network

```
SW-TOR-LAB(config)# ip route 10.127.96.0/24 10.127.98.2
```

Route from the PSK SSID to
the internal Aruba network

```
SW-TOR-LAB(config)# ip routing
```

```
SW-TOR-LAB(config)# snmp-server community aruba123 unrestricted
```

```
SW-TOR-LAB(config)# snmp-server host 10.127.88.20 community aruba123
```

```
SW-TOR-LAB(config)# password manager user-name admin plaintext  
aruba123
```

Configure SNMP

```
SW-TOR-LAB(config)# exit
```

```
SW-TOR-LAB # write memory
```

SW-Core

Virtual Switching Framework

The 5400R core switch used for this Mobile First VRD lab utilized Aruba's VSF feature. VSF technology virtualizes multiple physical devices into one virtual fabric which provides high availability due to significant reduction in recovery time simplified network design and management.

VSF allows supported switches connected to each other through Ethernet connections (copper or fiber) to behave like a single chassis switch.

Configuration guidelines:

- Supported for 5400R only (5406R, 5412R)
- 5400R with v3 modules, operating in v3-only mode
- Currently limited to 2 members (SW version 16.x.x or greater)
- Only same model switches can join a VSF system
- VSF links supported on 10G and 40G Ethernet interfaces only (no 1G)
- Each switch supports only 1 logical VSF link
- Logical VSF links can support up to 8 physical ports
- Physical ports can reside on different modules
- VSF is disabled on the switch by default

VSF provides the following advantages:

- Simplified topology and ease of management
- Single logical redundant entity
- VSF link aggregation
- Eliminates the need for L2 redundancy protocols such as spanning tree (STP)
- Eliminates the need for L3 redundancy protocols such as Virtual Routing Redundancy protocol (VRRP)

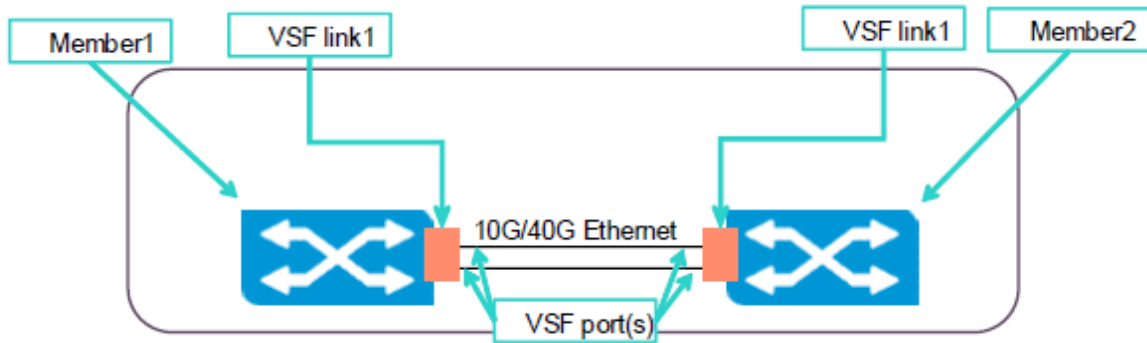


Figure 54 Basic VSF Topology

SW-Core VSF Configuration

5400-DC-Stack contains two physical HPE 5400R switches in a VSF. Firstly, this VSF must be set up. 5400-DCStack can then be treated as a single switch to configure the network settings. The following steps outline the process to setup VSF between dual 5400 switches.

1. Ensure both switches are in default configuration state. Issue an 'erase all' command on both switches

```
HP-Switch-5406Rz12# erase all
```

The system will be rebooted and all management module files except software images will be erased.

```
Continue (y/n)? y
```

2. On the 'primary' switch, set to v3-only mode and reload

```
HP-Switch-5406Rz12# config t
```

```
HP-Switch-5406Rz12(config)# no allow-v2-modules
```

This command will disable all V2 modules and reboot the switch.

```
Continue (y/n)? y
```

3. Add the ports (10 Gig or faster) as the VSF link and connect the switches together. Enable the VSF domain and reload. About one minute later, the second switch will automatically setup and reload.

```
HP-Switch-5406Rz12# config t
```

```
HP-Switch-5406Rz12(config)# vsf member 1 link 1 A23,A24
```

All configuration on this port has been removed and port is placed in VSF mode.

```
HP-Switch-5406Rz12(config)# vsf enable domain 1
```

4. After both switches reboot, confirm that VSF was successfully set up. The following is an example of the 5400-DC-Stack VSF configuration confirmation.

```
HP-VSF-Switch# show vsf
VSF Domain ID      : 1
MAC Address        : 5820b1-b3313f
VSF Topology       : Chain
VSF Status         : Active
Uptime             : 0d 0h 22m
VSF MAD            : None
VSF Port Speed     : 10G
Software Version   : KB.16.04.0009
Mbr
ID  Mac Address  Model                               Pri Status
---  -
1   941882-ce6b00 HP J9850A Switch 5406Rz12 128 Commander
2   941882-ce0e00 HP J9850A Switch 5406Rz12 128 Standby

HP-VSF-Switch# show vsf link detail
VSF Member: 1      Link: 1

Vsf-Port Port-State
-----
1/A23    Up: Connected to port 2/A23
1/A24    Up: Connected to port 2/A24

VSF Member: 2      Link: 1

Vsf-Port Port-State
-----
2/A23    Up: Connected to port 1/A23
2/A24    Up: Connected to port 1/A24

HP-VSF-Switch# write memory
```

SW-Core Remaining Configuration

```
SW-Core# configure terminal
```

Enter configuration mode

```
SW-Core(config)# hostname SW-Core
```

Change the hostname

```
SW-Core(config)# trunk 1/A7,2/A7 trk1 lacp  
SW-Core(config)# trunk 1/A1,2/A1 trk11 lacp  
SW-Core(config)# trunk 1/A2,2/A2 trk12 lacp  
SW-Core(config)# trunk 1/A3,2/A3 trk13 lacp  
SW-Core(config)# trunk 1/A4,2/A4 trk14 lacp  
SW-Core(config)# trunk 1/A8,2/A8 trk21 lacp
```

Add ports into 6 LAGs

```
SW-Core(config)# vlan 89  
SW-Core(vlan-89)# name 89-Servers  
SW-Core(vlan-89)# tagged Trk1  
SW-Core(vlan-89)# ip address 10.127.89.1 255.255.255.0  
SW-Core(vlan-89)# exit
```

Add VLAN 89 for Servers with ip address tagged on Trk1

```
SW-Core(config)# vlan 90  
SW-Core(vlan-90)# name 90-MobilityControllerMgmt  
SW-Core(vlan-90)# untagged Trk11-Trk14  
SW-Core(vlan-90)# ip address 10.127.90.1 255.255.255.0  
SW-Core(vlan-90)# exit
```

Add VLAN 90 for controller management with ip address untagged on Trk11, Trk12, Trk13, and Trk14

```
SW-Core(config)# vlan 91  
SW-Core(vlan-91)# name 91-SwitchMgmt  
SW-Core(vlan-91)# untagged Trk21  
SW-Core(vlan-91)# ip address 10.127.91.1 255.255.255.0  
SW-Core(vlan-91)# exit
```

Add VLAN 91 for switch management with ip address untagged on Trk21

```
SW-Core(config)# vlan 92  
SW-Core(vlan-92)# name 92-AccessPoint  
SW-Core(vlan-92)# tagged Trk21  
SW-Core(vlan-92)# ip address 10.127.92.1 255.255.255.0  
SW-Core(vlan-92)# jumbo  
SW-Core(vlan-92)# exit
```

Add VLAN 92 for APs with ip address as a jumbo VLAN tagged on Trk21

```
SW-Core(config)# vlan 95  
SW-Core(vlan-95)# name 95-ByodClients  
SW-Core(vlan-95)# tagged Trk11-Trk14
```

Add VLAN 95 for clients on the BYOD SSID with ip address tagged on Trk11,

```
SW-Core(vlan-95)# ip address 10.127.95.1 255.255.255.0
SW-Core(vlan-95)# ip helper-address 10.127.3.11
SW-Core(vlan-95)# exit
```

Trk12, Trk13, and Trk14 with DHCP helper address

```
SW-Core(config)# vlan 96
SW-Core(vlan-96)# name 96-PskClients
SW-Core(vlan-96)# tagged Trk11-Trk14
SW-Core(vlan-96)# ip address 10.127.96.1 255.255.255.0
SW-Core(vlan-95)# ip helper-address 10.127.3.11
SW-Core(vlan-96)# exit
```

Add VLAN 96 for clients on the PSK SSID with ip address tagged on Trk11, Trk12, Trk13, and Trk14 with DHCP helper address

```
SW-Core(config)# vlan 98
SW-Core(vlan-98)# name 98-Interconnect_Core-to-TOR
SW-Core(vlan-98)# untagged Trk1
SW-Core(vlan-98)# ip address 10.127.98.2 255.255.255.0
SW-Core(vlan-98)# exit
```

Add VLAN 98 for connectivity to the TOR switch with ip address untagged on Trk1 with DHCP helper address

```
SW-Core(config)# ip route 0.0.0.0 0.0.0.0 10.127.98.1
```

Create a default route from the Core switch to the TOR switch

```
SW-Core(config)# ip routing
```

```
SW-Core(config)# snmp-server community aruba123 unrestricted
SW-Core(config)# snmp-server host 10.127.88.20 community aruba123
SW-Core(config)# password manager user-name admin plaintext aruba123
SW-Core(config)# exit
```

Configure SNMP

```
SW-Core# write memory
```

SW-Access-01

```
Aruba-3810M-40G-8SR-PoEP-1-slot# configure
```

Enter configuration mode

```
SW-Access-01(config)# hostname SW-Access-01
```

Change the hostname

```
SW-Access-01(config)# trunk 1-2 Trk1 lacp
```

Add ports into a LAG

```
SW-Access-01(config)# vlan 91
```

```
SW-Access-01(vlan-91)# name 91-SwitchMgmt
```

```
SW-Access-01(vlan-91)# untagged Trk1
```

```
SW-Access-01(vlan-91)# ip address 10.127.91.101 255.255.255.0
```

```
SW-Access-01(vlan-91)# exit
```

Add VLAN 91 for switch management with ip address untagged on Trk1

```
SW-Access-01(config)# vlan 92
```

```
SW-Access-01(vlan-92)# name 92-AccessPoint
```

```
SW-Access-01(vlan-92)# untagged 3-48
```

```
SW-Access-01(vlan-92)# tagged Trk1
```

```
SW-Access-01(vlan-92)# exit
```

Add VLAN 92 for AP management untagged on ports 3-48 and tagged on Trk1

```
SW-Access-01(config)# ip default-gateway 10.127.91.1
```

Set the default gateway

```
SW-Access-01(config)# snmp-server community aruba123 unrestricted
```

Configure SNMP

```
SW-Access-01(config)# snmp-server host 10.127.88.20 community aruba123
```

```
SW-Access-01(config)# password manager user-name admin plaintext aruba123
```

```
SW-Access-01(config)# exit
```

```
SW-Access-01# write memory
```


MM-01 Initial Setup

```
Enter System name [ArubaMM-VA]: mm01
Enter Controller VLAN ID [1]: 89
Enter Controller VLAN port [GE 0/0/0]: GE 0/0/0
Enter Controller VLAN port mode (access|trunk) [access]: access
Enter VLAN interface IP address [172.16.0.254]: 10.127.89.11
Enter VLAN interface subnet mask [255.255.255.0]: 255.255.255.0
Enter IP Default gateway [none]: 10.127.89.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Enter Country code (ISO-3166), <ctrl-I> for supported list: us
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Los_Angeles
Enter Time in UTC [02:18:05]:
Enter Date (MM/DD/YYYY) [5/4/2018]: 06/18/2018
Enter Password for admin login (up to 32 chars): *****
Re-type Password for admin login: *****
```

Current choices are:

```
System name: mm01
Controller VLAN id: 89
Controller VLAN port: GE 0/0/0
Controller VLAN port mode: access
VLAN interface IP address: 10.127.89.11
VLAN interface subnet mask: 255.255.255.0
IP Default gateway: 10.127.89.1
Option to configure VLAN interface IPV6 address: no
Country code: us
IANA Time Zone: America/Los_Angeles
```

```
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
```

System will now restart!

MM-02 Initial Setup

```
Enter System name [ArubaMM-VA]: mm02
Enter Controller VLAN ID [1]: 89
Enter Controller VLAN port [GE 0/0/0]: GE 0/0/0
Enter Controller VLAN port mode (access|trunk) [access]: access
Enter VLAN interface IP address [172.16.0.254]: 10.127.89.12
Enter VLAN interface subnet mask [255.255.255.0]: 255.255.255.0
Enter IP Default gateway [none]: 10.127.89.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Enter Country code (ISO-3166), <ctrl-I> for supported list: us
You have chosen Countr06/18/2018y code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Los_Angeles
Enter Time in UTC [02:18:05]:
Enter Date (MM/DD/YYYY) [5/4/2018]:
Enter Password for admin login (up to 32 chars): *****
Re-type Password for admin login: *****
```

Current choices are:

```
System name: mm02
Controller VLAN id: 89
Controller VLAN port: GE 0/0/0
Controller VLAN port mode: access
VLAN interface IP address: 10.127.89.12
VLAN interface subnet mask: 255.255.255.0
IP Default gateway: 10.127.89.1
Option to configure VLAN interface IPV6 address: no
Country code: us
IANA Time Zone: America/Los_Angeles
```

```
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
```

System will now restart!

MM-01 Redundancy

```
(mm01) [mynode] #configure terminal
```

Enter configuration mode

```
(mm01) [mynode] (config) #vrrp 89
(mm01) ^[mynode] (config-submode) #description 89-MM-Redundancy
(mm01) ^[mynode] (config-submode) #ip address 10.127.89.10
(mm01) ^[mynode] (config-submode) #vlan 89
(mm01) ^[mynode] (config-submode) #priority 100
(mm01) ^[mynode] (config-submode) #no shutdown
(mm01) ^[mynode] (config-submode) #exit
```

Create VRRP instance 89 with virtual ip address and priority 100

```
(mm01) ^[mynode] (config) #cd /mm/mynode
(mm01) ^[mynode] (config) #master-redundancy
(mm01) ^[mynode] (config-submode) #master-vrrp 89
(mm01) ^[mynode] (config-submode) #peer-ip-address 10.127.89.12
ipsec aruba123
```

Configure master redundancy for VRRP instance 89 with MM-02

```
(mm01) ^[mynode] (config-submode) #exit
(mm01) ^[mynode] (config) #write memory
```

Saving Configuration...

Partial configuration for /mm/mynode

Contents of : /flash/ccm/partial/1/p=sc=mynode.cfg

vrrp 89

```
    ip address 10.127.89.10
    description 89-MM-Redundancy
    priority 100
    vlan 89
    no shutdown
```

!

master-redundancy

```
    master-vrrp 89
```

```
    peer-ip-address 10.127.89.12 ipsec ba1583e9b1bf79b7e8e4e021e0ed0c5c13cf9b0aaa3af656
```

!

Configuration Saved.

MM-02 Redundancy

```
(mm01) [mynode] #configure terminal
```

Enter configuration mode

```
(mm02) [mynode] (config) #vrrp 89
(mm02) ^[mynode] (config-submode) #description 89-MM-Redundancy
(mm02) ^[mynode] (config-submode) #ip address 10.127.89.10
(mm02) ^[mynode] (config-submode) #vlan 89
(mm02) ^[mynode] (config-submode) #priority 100
(mm02) ^[mynode] (config-submode) #no shutdown
(mm02) ^[mynode] (config-submode) #exit
```

Create VRRP instance 89 with virtual ip address and priority 100

```
(mm02) ^[mynode] (config) #cd /mm/mynode
(mm02) ^[mynode] (config) #master-redundancy
(mm02) ^[mynode] (config-submode) #master-vrrp 89
(mm02) ^[mynode] (config-submode) #peer-ip-address 10.127.89.11
ipsec aruba123
```

Configure master redundancy for VRRP instance 89 with MM-01

```
(mm02) ^[mynode] (config-submode) #exit
```

```
(mm02) ^[mynode] (config) #write memory
```

Saving Configuration...

Partial configuration for /mm/mynode

Contents of : /flash/ccm/partial/1/p=sc=mynode.cfg

```
vrrp 89
    ip address 10.127.89.10
    description 89-MM-Redundancy
    priority 100
    vlan 89
    no shutdown
!
master-redundancy
    master-vrrp 89
    peer-ip-address 10.127.89.11 ipsec fb871cf3a675e00c07e947912d86ccdd85808916fe2976ae
!
Configuration Saved.
```

MM-01 Licenses

Add License Keys

```
(mm01) [mynode] #cd /mm
```

Select the /mm level of the configuration hierarchy

```
(mm01) [mm] #configure terminal
```

Enter configuration mode

```
(mm01) [mm] (config) #license add Zs6/FfAq-3oNoYQsB-+k+JBdk9-  
B2ZbbfwE-1eDp/BoP-ebrtF//n-rcpQhCak-1T01XgrS-AM5ND+H4-2BM  
Limits updated.
```

Add the MM-VA license

```
(mm01) [mm] (config) #license add WfBAFcN3-zPdZr8cG-WcJYpWbX-  
I13zL277-zxy8NX7Q-oxstTo0y-t+J9ioDF-Zfm+91Mf-STboKrFO-2bk
```

Add the LIC-AP license

```
The limit for Access Points has been constrained to the platform  
limit [499]
```

```
(mm01) [mm] (config) #license add ljrSk1hn-TabYS001-VYN86W95-  
7/d011wr-HH4yjYq/-3P0zwReC-BzyU04go-7PIJ1ZKO-0vu01cjs-OtY
```

Add the LIC-PEF license (Policy Enforcement Firewall)

```
Please make sure to enable the feature bit to have the license  
take effect.
```

```
(mm01) [mm] (config) #license add ++CJGGtV-w4HfSCma-5s9lgR3s-  
mNwVVGNO-LOHvgVYY-4fh1MhTY-Gy8OfgYq-tEIn6Zn1-s5b7S0wf-KBI
```

Add the LIC-RFP license (RF Protect)

```
Please make sure to enable the feature bit to have the license  
take effect.
```

```
(mm01) [mm] (config) #license add npMVaDJ1-sgXS/PLo-noI9Rnis-  
RQPAJ10m-363eANDJ-UBDYlc6x-rFByHqbD-N4nZwY4Z-dXntPFxu-qcQ
```

Add the SUBX-WebCC license (Web Content Classification)

```
Please make sure to enable the feature bit to have the license  
take effect.
```

Enable License Feature Bits

All feature-based licenses must have their feature bits enabled in order for them to function. The configuration for this enablement in our validated reference design lab example is shown below:

```
(mm01) [mm] (config) #license-pool-profile-root
```

Enter configuration mode for the license pool profile at the root (/) level

```
(mm01) ^[mm] (License root(/) pool profile) #pefng-licenses-enable
```

Enable the LIC-PEF license feature bit

Please ensure to add licenses before enabling feature bit.

```
(mm01) ^[mm] (License root(/) pool profile) #rfp-license-enable
```

Enable the LIC-RFP license feature bit

Please ensure to add licenses before enabling feature bit.

```
(mm01) ^[mm] (License root(/) pool profile) #webcc-license-enable
```

Enable the SUBX-WebCC license feature bit

Please ensure to add licenses before enabling feature bit.

```
(mm01) ^[mm] (License root(/) pool profile) #exit
```

```
(mm01) ^[mm] (config) #write memory
```



The device is reaching out to receive updates for WebCC must have internet access.

MC-01 Initial Setup

Auto-provisioning is in progress. It requires DHCP and Activate servers

Choose one of the following options to override or debug auto-provisioning...

```
'enable-debug'      : Enable auto-provisioning debug logs
'disable-debug'     : Disable auto-provisioning debug logs
'mini-setup'        : Start mini setup dialog. Provides minimal customization and
requires DHCP server
'full-setup'        : Start full setup dialog. Provides full customization
'static-activate'   : Provides customization for static or PPPoE ip assignment. Uses
activate for master information
```

Enter Option (partial string is acceptable): **full-setup**

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no):
yes

```
***** Welcome to the Aruba7210 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.
```

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

```
Enter System name [Aruba7210]: mc01
Enter Switch Role (master|standalone|md) [md]: md
Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]: ipv4
Enter Master switch IP address or FQDN: 10.127.89.10
Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]: no
This device connects to Master switch via VPN concentrator (yes|no) [no]: no
Is Master switch Virtual Mobility Master? (yes|no) [yes]: yes
Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]: PSKwithIP
Enter IPSec Pre-shared Key: aruba123
Re-enter IPSec Pre-shared Key: aruba123
Do you want to enable L3 Redundancy (yes|no) [no]: no
Enter Uplink Vlan ID [1]: 90
Enter Uplink port [GE 0/0/0]: GE 0/0/0
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 90
Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]: static
Enter Uplink Vlan Static IP address [172.16.0.254]: 10.127.90.11
Enter Uplink Vlan Static IP netmask [255.255.255.0]: 255.255.255.0
Enter IP default gateway [none]: 10.127.90.1
Enter DNS IP address [none]: 10.127.3.11
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
```

```
Do you want to configure dynamic port-channel (yes|no) [no]: yes
Enter Port-channel ID [0]: 0
This controller is restricted, please enter country code (US|PR|GU|VI|MP|AS|FM|MH) [US]: US
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Los_Angeles
Enter Time in UTC [02:50:51]:
Enter Date (MM/DD/YYYY) [5/4/2018]:
Do you want to create admin account (yes|no) [yes]: yes
Enter Password for admin login (up to 32 chars): aruba123
Re-type Password for admin login: aruba123
```

Current choices are:

```
System name: mc01
Switch Role: md
IP type to terminate IPsec tunnel: ipv4
Master switch IP address or FQDN: 10.127.89.10
Is this VPN concentrator: no
Connect via VPN concentrator: no
IPsec authentication method: PSKwithIP
Vlan id for uplink interface: 90
Uplink port: GE 0/0/0
Uplink port mode: trunk
Native VLAN id: 90
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 10.127.90.11
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 10.127.90.1
Domain Name Server to resolve FQDN: 10.127.3.11
Option to configure VLAN interface IPV6 address: no
PC ID for uplink: 0
Country code: US
IANA Time Zone: America/Los_Angeles
Admin account created: yes
```

Note: These settings require IP-Based-PSK configuration on Master switch

```
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no) yes
```


MC-02 Initial Setup

Auto-provisioning is in progress. It requires DHCP and Activate servers

Choose one of the following options to override or debug auto-provisioning...

```
'enable-debug'      : Enable auto-provisioning debug logs
'disable-debug'     : Disable auto-provisioning debug logs
'mini-setup'        : Start mini setup dialog. Provides minimal customization and
requires DHCP server
'full-setup'        : Start full setup dialog. Provides full customization
'static-activate'   : Provides customization for static or PPPoE ip assignment. Uses
activate for master information
```

Enter Option (partial string is acceptable): **full-setup**

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no):
yes

```
***** Welcome to the Aruba7210 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.
```

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

```
Enter System name [Aruba7210]: mc02
Enter Switch Role (master|standalone|md) [md]: md
Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]: ipv4
Enter Master switch IP address or FQDN: 10.127.89.10
Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]: no
This device connects to Master switch via VPN concentrator (yes|no) [no]: no
Is Master switch Virtual Mobility Master? (yes|no) [yes]: yes
Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]: PSKwithIP
Enter IPSec Pre-shared Key: aruba123
Re-enter IPSec Pre-shared Key: aruba123
Do you want to enable L3 Redundancy (yes|no) [no]: no
Enter Uplink Vlan ID [1]: 90
Enter Uplink port [GE 0/0/0]: GE 0/0/0
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 90
Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]: static
Enter Uplink Vlan Static IP address [172.16.0.254]: 10.127.90.12
Enter Uplink Vlan Static IP netmask [255.255.255.0]: 255.255.255.0
Enter IP default gateway [none]: 10.127.90.1
Enter DNS IP address [none]: 10.127.3.11
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
```

```
Do you want to configure dynamic port-channel (yes|no) [no]: yes
Enter Port-channel ID [0]: 0
This controller is restricted, please enter country code (US|PR|GU|VI|MP|AS|FM|MH) [US]: US
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Los_Angeles
Enter Time in UTC [02:50:51]:
Enter Date (MM/DD/YYYY) [5/4/2018]:
Do you want to create admin account (yes|no) [yes]: yes
Enter Password for admin login (up to 32 chars): aruba123
Re-type Password for admin login: aruba123
```

Current choices are:

```
System name: mc02
Switch Role: md
IP type to terminate IPsec tunnel: ipv4
Master switch IP address or FQDN: 10.127.89.10
Is this VPN concentrator: no
Connect via VPN concentrator: no
IPsec authentication method: PSKwithIP
Vlan id for uplink interface: 90
Uplink port: GE 0/0/0
Uplink port mode: trunk
Native VLAN id: 90
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 10.127.90.12
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 10.127.90.1
Domain Name Server to resolve FQDN: 10.127.3.11
Option to configure VLAN interface IPV6 address: no
PC ID for uplink: 0
Country code: US
IANA Time Zone: America/Los_Angeles
Admin account created: yes
```

Note: These settings require IP-Based-PSK configuration on Master switch

```
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no) yes
```

MC-03 Initial Setup

Auto-provisioning is in progress. It requires DHCP and Activate servers

Choose one of the following options to override or debug auto-provisioning...

```
'enable-debug'      : Enable auto-provisioning debug logs
'disable-debug'     : Disable auto-provisioning debug logs
'mini-setup'        : Start mini setup dialog. Provides minimal customization and
requires DHCP server
'full-setup'        : Start full setup dialog. Provides full customization
'static-activate'   : Provides customization for static or PPPoE ip assignment. Uses
activate for master information
```

Enter Option (partial string is acceptable): **full-setup**

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no):
yes

```
***** Welcome to the Aruba7210 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.
```

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

```
Enter System name [Aruba7210]: mc03
Enter Switch Role (master|standalone|md) [md]: md
Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]: ipv4
Enter Master switch IP address or FQDN: 10.127.89.10
Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]: no
This device connects to Master switch via VPN concentrator (yes|no) [no]: no
Is Master switch Virtual Mobility Master? (yes|no) [yes]: yes
Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]: PSKwithIP
Enter IPSec Pre-shared Key: aruba123
Re-enter IPSec Pre-shared Key: aruba123
Do you want to enable L3 Redundancy (yes|no) [no]: no
Enter Uplink Vlan ID [1]: 90
Enter Uplink port [GE 0/0/0]: GE 0/0/0
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 90
Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]: static
Enter Uplink Vlan Static IP address [172.16.0.254]: 10.127.90.13
Enter Uplink Vlan Static IP netmask [255.255.255.0]: 255.255.255.0
Enter IP default gateway [none]: 10.127.90.1
Enter DNS IP address [none]: 10.127.3.11
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
```

```
Do you want to configure dynamic port-channel (yes|no) [no]: yes
Enter Port-channel ID [0]: 0
This controller is restricted, please enter country code (US|PR|GU|VI|MP|AS|FM|MH) [US]: US
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Los_Angeles
Enter Time in UTC [02:50:51]:
Enter Date (MM/DD/YYYY) [5/4/2018]:
Do you want to create admin account (yes|no) [yes]: yes
Enter Password for admin login (up to 32 chars): aruba123
Re-type Password for admin login: aruba123
```

Current choices are:

```
System name: mc03
Switch Role: md
IP type to terminate IPsec tunnel: ipv4
Master switch IP address or FQDN: 10.127.89.10
Is this VPN concentrator: no
Connect via VPN concentrator: no
IPsec authentication method: PSKwithIP
Vlan id for uplink interface: 90
Uplink port: GE 0/0/0
Uplink port mode: trunk
Native VLAN id: 90
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 10.127.90.13
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 10.127.90.1
Domain Name Server to resolve FQDN: 10.127.3.11
Option to configure VLAN interface IPV6 address: no
PC ID for uplink: 0
Country code: US
IANA Time Zone: America/Los_Angeles
Admin account created: yes
```

Note: These settings require IP-Based-PSK configuration on Master switch

```
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no) yes
```

MC-04 Initial Setup

Auto-provisioning is in progress. It requires DHCP and Activate servers

Choose one of the following options to override or debug auto-provisioning...

```
'enable-debug'      : Enable auto-provisioning debug logs
'disable-debug'     : Disable auto-provisioning debug logs
'mini-setup'        : Start mini setup dialog. Provides minimal customization and
requires DHCP server
'full-setup'        : Start full setup dialog. Provides full customization
'static-activate'   : Provides customization for static or PPPoE ip assignment. Uses
activate for master information
```

Enter Option (partial string is acceptable): **full-setup**

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no):
yes

```
***** Welcome to the Aruba7210 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.
```

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

```
Enter System name [Aruba7210]: mc04
Enter Switch Role (master|standalone|md) [md]: md
Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]: ipv4
Enter Master switch IP address or FQDN: 10.127.89.10
Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]: no
This device connects to Master switch via VPN concentrator (yes|no) [no]: no
Is Master switch Virtual Mobility Master? (yes|no) [yes]: yes
Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]: PSKwithIP
Enter IPSec Pre-shared Key: aruba123
Re-enter IPSec Pre-shared Key: aruba123
Do you want to enable L3 Redundancy (yes|no) [no]: no
Enter Uplink Vlan ID [1]: 90
Enter Uplink port [GE 0/0/0]: GE 0/0/0
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 90
Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]: static
Enter Uplink Vlan Static IP address [172.16.0.254]: 10.127.90.14
Enter Uplink Vlan Static IP netmask [255.255.255.0]: 255.255.255.0
Enter IP default gateway [none]: 10.127.90.1
Enter DNS IP address [none]: 10.127.3.11
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
```

```
Do you want to configure dynamic port-channel (yes|no) [no]: yes
Enter Port-channel ID [0]: 0
This controller is restricted, please enter country code (US|PR|GU|VI|MP|AS|FM|MH) [US]: US
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Los_Angeles
Enter Time in UTC [02:50:51]:
Enter Date (MM/DD/YYYY) [5/4/2018]:
Do you want to create admin account (yes|no) [yes]: yes
Enter Password for admin login (up to 32 chars): aruba123
Re-type Password for admin login: aruba123
```

Current choices are:

```
System name: mc04
Switch Role: md
IP type to terminate IPsec tunnel: ipv4
Master switch IP address or FQDN: 10.127.89.10
Is this VPN concentrator: no
Connect via VPN concentrator: no
IPsec authentication method: PSKwithIP
Vlan id for uplink interface: 90
Uplink port: GE 0/0/0
Uplink port mode: trunk
Native VLAN id: 90
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 10.127.90.14
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 10.127.90.1
Domain Name Server to resolve FQDN: 10.127.3.11
Option to configure VLAN interface IPV6 address: no
PC ID for uplink: 0
Country code: US
IANA Time Zone: America/Los_Angeles
Admin account created: yes
```

Note: These settings require IP-Based-PSK configuration on Master switch

```
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no) yes
```

MM-01 Remaining Configuration

```
(mm01) [mm] (config) #cd /mm
```

Navigate to the Mobility Master node

```
(mm01) [mm] (config) #database synchronize period 60
```

Adjust the database synchronization period

```
(mm01) ^[mm] (config) #write memory
```

```
(mm01) [mm] (config) #configuration node /md/Aruba
```

```
(mm01) [mm] (config) #configuration node /md/Aruba/campus
```

Create the /md/aruba and /md/aruba/campus nodes

```
(mm01) [mm] (config) #cd /mm
```

```
(mm01) [mm] (config) #localip 10.127.90.11 ipsec aruba123
```

Configure secure communication between MM-01 and MC-01

```
(mm01) ^[mm] (config) #localip 10.127.90.12 ipsec aruba123
```

Configure secure communication between MM-01 and MC-02

```
(mm01) ^[mm] (config) #localip 10.127.90.13 ipsec aruba123
```

Configure secure communication between MM-01 and MC-03

```
(mm01) ^[mm] (config) #localip 10.127.90.14 ipsec aruba123
```

Configure secure communication between MM-01 and MC-04

```
(mm01) ^[mm] (config) #write memory
```

```
(mm01) [mm] (config) #configuration device 00:1a:1e:01:a9:a0  
device-model A7210 /md/aruba/campus
```

Add MC-01 to the /md/aruba/campus node

```
(mm01) [mm] (config) #configuration device 00:1a:1e:00:73:c0  
device-model A7210 /md/aruba/campus
```

Add MC-02 to the /md/aruba/campus node

```
(mm01) [mm] (config) #configuration device 00:1a:1e:03:7c:d8  
device-model A7210 /md/aruba/campus
```

Add MC-03 to the /md/aruba/campus node

```
(mm01) [mm] (config) #configuration device 00:1a:1e:03:7d:b8  
device-model A7210 /md/aruba/campus
```

Add MC-04 to the /md/aruba/campus node



Wait for the tunnels to be built between the MCs and the MM before proceeding with the configuration.

```
(mm01) [mm] (config) #cd /mm
(mm01) [mm] (config) #ntp server 10.127.32.10
```

Designate NTP, SNMP,
and AirWave servers for
MM-01

```
(mm01) ^[mm] (config) #snmp-server community aruba123
(mm01) ^[mm] (config) #snmp-server host 10.127.88.20 version 2c
aruba123
(mm01) ^[mm] (config) #mgmt-server primary-server 10.127.88.20
profile default-amp
(mm01) ^[mm] (config) #write memory
```

```
(mm01) [mm] (config) #cd /md/Aruba
```

Navigate to the Aruba
node

```
(mm01) [Aruba] (config) #ntp server 10.127.32.10
(mm01) ^[Aruba] (config) #snmp-server community aruba123
```

Designate servers for all
devices managed by
MM-01

```
(mm01) ^[Aruba] (config) #snmp-server host 10.127.88.20 version 2c
aruba123
(mm01) ^[md Aruba] (config) #mgmt-server primary-server 10.127.88.20
profile default-amp
```

```
(mm01) ^[Aruba] (config) #firewall-visibility
(mm01) ^[Aruba] (config) #firewall
```

Add firewall visibility to
enable monitoring on
MDs

```
(mm01) ^[Aruba] (config-submode)#dpi
```

Warning: Application visibility/control is enabled, this change would take effect after reloading the controller(s) in "/md/Aruba"

```
(mm01) ^[Aruba] (config-submode) #web-cc
(mm01) ^[Aruba] (config-submode) #exit
(mm01) ^[Aruba] (config) #write memory
```

```
(mm01) [Aruba] (config) #cd /md/aruba/campus
```

Navigate to the Campus group

```
(mm01) [campus] (config) #vlan 90
(mm01) ^[campus] (config-submode) #description 90-MobilityControllers
(mm01) ^[campus] (config-submode) #exit
```

Add VLAN 90 for Mobility
Controller management

```
(mm01) ^[campus] (config) #vlan 95
(mm01) ^[campus] (config-submode) #description 95-ByodClients
(mm01) ^[campus] (config-submode) #exit
```

Add VLAN 95 for BYOD
clients

```
(mm01) ^[campus] (config) #vlan 96
(mm01) ^[campus] (config-submode) #description 96-PskClients
(mm01) ^[campus] (config-submode) #exit
```

Add VLAN 96 for PSK
clients


```
(mm01) ^[campus] (config) #interface gigabitethernet 0/0/0
(mm01) ^[campus] (config-submode) #lldp transmit
(mm01) ^[campus] (config-submode) #lldp receive
(mm01) ^[campus] (config-submode) #lACP group 0 mode active
(mm01) ^[campus] (config-submode) #exit
```

Define LAG settings for all MCs under the Campus group

```
(mm01) ^[campus] (config) #interface gigabitethernet 0/0/1
(mm01) ^[campus] (config-submode) #lldp transmit
(mm01) ^[campus] (config-submode) #lldp receive
(mm01) ^[campus] (config-submode) #lACP group 0 mode active
(mm01) ^[campus] (config-submode) #exit
```

```
(mm01) ^[campus] (config) #interface port-channel 0
(mm01) ^[campus] (config-submode) #switchport mode trunk
(mm01) ^[campus] (config-submode) #switchport trunk allowed vlan 90,95,96
(mm01) ^[campus] (config-submode) #switchport trunk native vlan 90
Configuration will take effect after VLAN is created
(mm01) ^[campus] (config-submode) #exit
(mm01) ^[campus] (config) #write memory
```

```
(mm01) [campus] (config) #cd /md/aruba/campus/00:1a:1e:01:a9:a0
```

Navigate to MC-01

```
(mm01) [00:1a:1e:01:a9:a0] (config) #interface gigabitethernet 0/0/0
(mm01) [00:1a:1e:01:a9:a0] (config-submode) #no lACP group
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #interface port-channel 0
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #no switchport mode
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #no switchport trunk allowed vlan
Config deletion will not take effect: configuration is inherited.
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #no switchport trunk native vlan
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #exit
```

Remove startup wizard settings from device level configuration

```
(mm01) ^[00:1a:1e:01:a9:a0] (config) #interface vlan 95
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #ip address 10.127.95.11
255.255.255.0
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #exit
```

Define ip address for MC-01 on VLAN 95 for BYOD clients

```
(mm01) ^[00:1a:1e:01:a9:a0] (config) #interface vlan 96
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #ip address 10.127.96.11
255.255.255.0
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #exit
```

Define ip address for MC-01 on VLAN 96 for PSK clients

```
(mm01) ^[00:1a:1e:01:a9:a0] (config) #write memory
```

```
(mm01) [00:1a:1e:01:a9:a0] (config) #cd  
/md/aruba/campus/00:1a:1e:00:73:c0
```

Navigate to MC-02

```
(mm01) [00:1a:1e:00:73:c0] (config) #interface gigabitethernet 0/0/0  
(mm01) [00:1a:1e:00:73:c0] (config-submode) #no lACP group  
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #interface port-channel  
0
```

Remove startup wizard settings from device level configuration

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #no switchport mode  
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #no switchport trunk  
allowed vlan
```

Config deletion will not take effect: configuration is inherited.

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #no switchport trunk  
native vlan
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #exit
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config) #interface vlan 95
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #ip address 10.127.95.12  
255.255.255.0
```

Define ip address for MC-02 on VLAN 95 for BYOD clients

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #exit
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config) #interface vlan 96
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #ip address 10.127.96.12  
255.255.255.0
```

Define ip address for MC-02 on VLAN 96 for PSK clients

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #exit
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config) #write memory
```

```
(mm01) [00:1a:1e:00:73:c0] (config) #cd  
/md/aruba/campus/00:1a:1e:03:7c:d8
```

Navigate to MC-03

```
(mm01) [00:1a:1e:03:7c:d8] (config) #interface gigabitethernet 0/0/0  
(mm01) [00:1a:1e:03:7c:d8] (config-submode) #no lACP group  
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #interface port-channel 0
```

Remove startup wizard settings from device level configuration

```
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #no switchport mode  
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #no switchport trunk allowed vlan
```

Config deletion will not take effect: configuration is inherited.

```
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #no switchport trunk native vlan
```

```
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #exit
```

```
(mm01) ^[00:1a:1e:03:7c:d8] (config) #interface vlan 95
```

Define ip address for MC-03 on VLAN 95 for BYOD clients

```
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #ip address 10.127.95.13 255.255.255.0
```

```
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #exit
```

```
(mm01) ^[00:1a:1e:03:7c:d8] (config) #interface vlan 96
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #ip address 10.127.96.13
255.255.255.0
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #exit
(mm01) ^[00:1a:1e:03:7c:d8] (config) #write memory
```

Define ip address for MC-03 on VLAN 96 for PSK clients

```
(mm01) [00:1a:1e:03:7c:d8] (config) #cd /md/aruba/campus/00:1a:1e:03:7d:b8
```

Navigate to MC-04

```
(mm01) [00:1a:1e:03:7d:b8] (config) #interface gigabitethernet 0/0/0
(mm01) [00:1a:1e:03:7d:b8] (config-submode) #no lacp group
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #interface port-channel 0
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #no switchport mode
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #no switchport trunk allowed vlan
Config deletion will not take effect: configuration is inherited.
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #no switchport trunk native vlan
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #exit
```

Remove startup wizard settings from device level configuration

```
(mm01) ^[00:1a:1e:03:7d:b8] (config) #interface vlan 95
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #ip address 10.127.95.14
255.255.255.0
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #exit
```

Define ip address for MC-04 on VLAN 95 for BYOD clients

```
(mm01) ^[00:1a:1e:03:7d:b8] (config) #interface vlan 96
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #ip address 10.127.96.14
255.255.255.0
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #exit
(mm01) ^[00:1a:1e:03:7d:b8] (config) #write memory
```

Define ip address for MC-04 on VLAN 96 for BYOD clients

```
(mm01) [00:1a:1e:03:7d:b8] (config) #cd /md/aruba/campus
```

Navigate to the Campus group

```
(mm01) [campus] (config) #lc-cluster group-profile campus-cluster
```

Create cluster profile

```
(mm01) ^[campus] (Classic Controller Cluster Profile "campus-cluster") #controller 10.127.90.11 vrrp-ip 10.127.90.21 vrrp-vlan 90
(mm01) ^[campus] (Classic Controller Cluster Profile "campus-cluster") #controller 10.127.90.12 vrrp-ip 10.127.90.22 vrrp-vlan 90
(mm01) ^[campus] (Classic Controller Cluster Profile "campus-cluster") #controller 10.127.90.13 vrrp-ip 10.127.90.23 vrrp-vlan 90
(mm01) ^[campus] (Classic Controller Cluster Profile "campus-cluster") #controller 10.127.90.14 vrrp-ip 10.127.90.24 vrrp-vlan 90
(mm01) ^[campus] (Classic Controller Cluster Profile "campus-cluster") #redundancy
(mm01) ^[campus] (Classic Controller Cluster Profile "campus-cluster") #active-ap-1b
(mm01) ^[campus] (Classic Controller Cluster Profile "campus-cluster") #exit
```

Configure cluster VRRP settings

```
(mm01) ^[campus] (config) #write memory
```

```
(mm01) [campus] (config) #cd /md/aruba/campus/00:1a:1e:01:a9:a0
```

Navigate to MC-01

```
(mm01) [00:1a:1e:01:a9:a0] (config) #lc-cluster group-membership  
campus-cluster
```

Configure device-specific VRRP settings for the cluster

```
(mm01) ^[00:1a:1e:01:a9:a0] (config) #lc-cluster exclude-vlan 1
```

```
(mm01) ^[00:1a:1e:01:a9:a0] (config) #vrrp 90
```

```
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #ip address 10.127.90.10
```

```
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #authentication aruba123
```

```
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #priority 255
```

```
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #advertise 1
```

```
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #vlan 90
```

```
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #no shutdown
```

```
(mm01) ^[00:1a:1e:01:a9:a0] (config-submode) #exit
```

```
(mm01) ^[00:1a:1e:01:a9:a0] (config) #write memory
```

```
(mm01) [00:1a:1e:01:a9:a0] (config) #cd /md/aruba/campus/00:1a:1e:00:73:c0
```

Navigate to MC-02

```
(mm01) [00:1a:1e:00:73:c0] (config) #lc-cluster group-membership  
campus-cluster
```

Configure device-specific VRRP settings for the cluster

```
(mm01) ^[00:1a:1e:00:73:c0] (config) #lc-cluster exclude-vlan 1
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config) #vrrp 90
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #ip address 10.127.90.10
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #authentication aruba123
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #priority 250
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #advertise 1
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #vlan 90
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #no shutdown
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config-submode) #exit
```

```
(mm01) ^[00:1a:1e:00:73:c0] (config) #write memory
```

```
(mm01) [00:1a:1e:00:73:c0] (config) #cd /md/aruba/campus/00:1a:1e:03:7c:d8
```

Navigate to MC-03

```
(mm01) [00:1a:1e:03:7c:d8] (config) #lc-cluster group-membership  
campus-cluster
```

Configure device-specific VRRP settings for the cluster

```
(mm01) ^[00:1a:1e:03:7c:d8] (config) #lc-cluster exclude-vlan 1
```

```
(mm01) ^[00:1a:1e:03:7c:d8] (config) #vrrp 90
```

```
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #ip address 10.127.90.10
```

```
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #authentication aruba123
```

```
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #priority 245
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #advertise 1
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #vlan 90
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #no shutdown
(mm01) ^[00:1a:1e:03:7c:d8] (config-submode) #exit
```

```
(mm01) ^[00:1a:1e:03:7c:d8] (config) #write memory
```

```
(mm01) [00:1a:1e:03:7c:d8] (config) #cd /md/aruba/campus/00:1a:1e:03:7d:b8
```

Navigate to MC-04

```
(mm01) [00:1a:1e:03:7d:b8] (config) #lc-cluster group-membership
campus-cluster
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config) #lc-cluster exclude-vlan 1
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config) #vrrp 90
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #ip address 10.127.90.10
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #authentication aruba123
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #priority 240
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #advertise 1
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #vlan 90
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #no shutdown
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config-submode) #exit
```

```
(mm01) ^[00:1a:1e:03:7d:b8] (config) #write memory
```

Configure device-specific VRRP settings for the cluster

Employee BYOD SSID Configuration

```
(mm01) #configure terminal
```

Enter configuration mode

Enter Configuration commands, one per line. End with CNTL/Z

```
(mm01) (config) #cd /md/aruba
```

Permit access for BYOD clients to the captive portal

```
(mm01) [aruba] (config) #ip access-list session mobilefirst-allow-captiveportal
```

```
(mm01) ^[aruba] (config-submode) #user host 10.127.89.30 svc-http permit
```

```
(mm01) ^[aruba] (config-submode) #user host 10.127.89.30 svc-https permit
```

```
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config) #ip access-list session MobileFirst-byod_employee-deny-client-as-dhcp-server
```

Prevent BYOD clients from acting as a DHCP server

```
(mm01) ^[aruba] (config-submode) #user any udp 68 deny
```

```
(mm01) ^[aruba] (config-submode) #ipv6 user any icmpv6 rtr-adv deny
```

```
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config) #ip access-list session MobileFirst-byod_employee-allowall
```

Allow all other traffic to and from BYOD clients

```
(mm01) ^[aruba] (config-submode) #any any any permit
```

```
(mm01) ^[aruba] (config-submode) #ipv6 any any any permit
```

```
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config) #user-role onboard
```

Create the onboard user role and apply the appropriate ACLs

```
(mm01) ^[aruba] (config-submode) #access-list session mobilefirst-allow-captiveportal position 3
```

```
(mm01) ^[aruba] (config-submode) #access-list session logon-control position 4
```

```
(mm01) ^[aruba] (config-submode) #access-list session captiveportal position 5
```

```
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config) #user-role Mobilefirst-byod_employee
```

Create the Mobilefirst-byod_employee user role and apply the appropriate ACLs

```
(mm01) ^[aruba] (config-submode) #access-list session MobileFirst-byod_employee-deny-client-as-dhcp-server
```

```
(mm01) ^[aruba] (config-submode) #access-list session MobileFirst-byod_employee-allowall
```

```
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config) #aaa authentication-server radius CP-Corp
```

Designate RADIUS server

```
(mm01) ^[aruba] (RADIUS Server "CP-Corp") #host 10.127.89.30
```

```
(mm01) ^[aruba] (RADIUS Server "CP-Corp") #key aruba123
```

```
(mm01) ^[aruba] (RADIUS Server "CP-Corp") #mac-delimiter colon
```

```
(mm01) ^[aruba] (RADIUS Server "CP-Corp") #exit
```

```
(mm01) ^[aruba] (config) #aaa rfc-3576-server 10.127.89.30
(mm01) ^[aruba] (RFC 3576 Server " 10.127.89.30") #key aruba123
(mm01) ^[aruba] (RFC 3576 Server " 10.127.89.30") #exit
```

Designate RFC 3576 server

```
(mm01) ^[aruba] (config) #aaa server-group CP-Corp
(mm01) ^[aruba] (Server Group "CP-Corp") #auth-server CP-Corp
(mm01) ^[aruba] (Server Group "CP-Corp") #exit
```

Define AAA server Group

```
(mm01) [aruba] (config) #aaa authentication dot1x MobileFirst-
byod_employee
```

Define 802.1X authentication profile

```
(mm01) [aruba] (802.1X Authentication Profile "MobileFirst-byod_employee") #exit
```

```
(mm01) ^[aruba] (config-submode) #aaa profile MobileFirst-
byod_employee
```

Define AAA profile for MobileFirst-byod_employee

```
(mm01) ^[aruba] (AAA Profile "MobileFirst-byod_employee") #initial-role onboard
(mm01) ^[aruba] (AAA Profile "MobileFirst-byod_employee") #dot1x-default-role onboard
(mm01) ^[aruba] (AAA Profile "MobileFirst-byod_employee") #rfc-3576-server 10.127.89.30
(mm01) ^[aruba] (AAA Profile "MobileFirst-byod_employee") #radius-accounting CP-Corp
(mm01) ^[aruba] (AAA Profile "MobileFirst-byod_employee") #authentication-dot1x
MobileFirst-byod_employee
(mm01) ^[aruba] (AAA Profile "MobileFirst-byod_employee") #dot1x-server-group CP-Corp
(mm01) ^[aruba] (AAA Profile "MobileFirst-byod_employee") #exit
```

```
(mm01) ^[aruba] (config) #netdestination GOOGLE-PLAY
(mm01) ^[aruba] (config-submode) #name *.gppht.com
(mm01) ^[aruba] (config-submode) #name *.gstatic.com
(mm01) ^[aruba] (config-submode) #name *.android.clients.google.com
(mm01) ^[aruba] (config-submode) #name *.accounts.google.com
(mm01) ^[aruba] (config-submode) #name *.clients1.google.com
(mm01) ^[aruba] (config-submode) #name *.clients2.google.com
(mm01) ^[aruba] (config-submode) #name *.clients3.google.com
(mm01) ^[aruba] (config-submode) #name *.clients4.google.com
(mm01) ^[aruba] (config-submode) #name *.i.ytimg.com
(mm01) ^[aruba] (config-submode) #name *.google-analytics.com
(mm01) ^[aruba] (config-submode) #name *.android.l.google.com
(mm01) ^[aruba] (config-submode) #name *.mtalk.google.com
(mm01) ^[aruba] (config-submode) #name *.clients.l.google.com
(mm01) ^[aruba] (config-submode) #name *.googleapis.com
(mm01) ^[aruba] (config-submode) #name *.play.google.com
(mm01) ^[aruba] (config-submode) #name *.1e100.net
(mm01) ^[aruba] (config-submode) #name *.gvt1.com
(mm01) ^[aruba] (config-submode) #name *.l.googleusercontent.com
(mm01) ^[aruba] (config-submode) #name *.gppht.net
```

Define Netdestination for GOOGLE-PLAY

```
(mm01) ^[aruba] (config-submode) #name android.clients.google.com
(mm01) ^[aruba] (config-submode) #name ggpht.com
(mm01) ^[aruba] (config-submode) #name gstatic.com
(mm01) ^[aruba] (config-submode) #name accounts.google.com
(mm01) ^[aruba] (config-submode) #name clients1.google.com
(mm01) ^[aruba] (config-submode) #name clients2.google.com
(mm01) ^[aruba] (config-submode) #name clients3.google.com
(mm01) ^[aruba] (config-submode) #name clients4.google.com
(mm01) ^[aruba] (config-submode) #name i.ytimg.com
(mm01) ^[aruba] (config-submode) #name google-analytics.com
(mm01) ^[aruba] (config-submode) #name android.l.google.com
(mm01) ^[aruba] (config-submode) #name mtalk.google.com
(mm01) ^[aruba] (config-submode) #name clients.l.google.com
(mm01) ^[aruba] (config-submode) #name googleapis.com
(mm01) ^[aruba] (config-submode) #name play.google.com
(mm01) ^[aruba] (config-submode) #name le100.net
(mm01) ^[aruba] (config-submode) #name gvt1.com
(mm01) ^[aruba] (config-submode) #name l.googleusercontent.com
(mm01) ^[aruba] (config-submode) #name ggpht.net
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config) #aaa authentication captive-portal
MobileFirst-onboard
```

Define captive portal profile

```
(mm01) ^[aruba] (Captive Portal Authentication Profile "MobileFirst-onboard") #white-list
GOOGLE-PLAY
(mm01) ^[aruba] (Captive Portal Authentication Profile "MobileFirst-onboard") #login-page
https://cp-corp.aruba-tme.com/onboard/byod_employee_onboard.php
(mm01) ^[aruba] (Captive Portal Authentication Profile "MobileFirst-onboard") # welcome-
page /auth/welcome.html
(mm01) ^[aruba] (Captive Portal Authentication Profile "MobileFirst-onboard") #no guest-
logon
(mm01) ^[aruba] (Captive Portal Authentication Profile "MobileFirst-onboard") #redirect-
pause 3
(mm01) ^[aruba] (Captive Portal Authentication Profile "MobileFirst-onboard") #server-group
CP-Corp
(mm01) ^[aruba] (Captive Portal Authentication Profile "MobileFirst-onboard") #default-role
onboard
(mm01) ^[aruba] (Captive Portal Authentication Profile "MobileFirst-onboard") #url-hash-key
aruba123
(mm01) ^[aruba] (Captive Portal Authentication Profile "MobileFirst-onboard") #exit
```

```
(mm01) ^[aruba] (config) #user-role onboard
(mm01) ^[aruba] (config-role) #captive-portal MobileFirst-onboard
(mm01) ^[aruba] (config-role) #exit
```

Add captive portal profile to the onboard user role


```
(mm01) [aruba] (config) #wlan ssid-profile MobileFirst-  
byod_employee
```

Define SSID profile for
MobileFirst-byod_employee

```
(mm01) ^[aruba] (SSID Profile "MobileFirst-byod_employee") #ssid "TME-MobileFirst-  
byod_employee"
```

```
(mm01) ^[aruba] (SSID Profile "MobileFirst-byod_employee") #opmode wpa2-aes
```

```
(mm01) ^[aruba] (SSID Profile "MobileFirst-byod_employee") #exit
```

```
(mm01) ^[aruba] (config) #wlan virtual-ap MobileFirst-  
byod_employee
```

Create the virtual AP profile
Add the AAA and SSID profiles
to the virtual AP profile

```
(mm01) ^[aruba] (Virtual AP profile "MobileFirst-byod_employee")  
#aaa-profile MobileFirst-byod_employee
```

```
(mm01) ^[aruba] (Virtual AP profile "MobileFirst-byod_employee") #ssid-profile MobileFirst-  
byod_employee
```

```
(mm01) ^[aruba] (Virtual AP profile "MobileFirst-byod_employee") #vlan 95
```

```
(mm01) ^[aruba] (Virtual AP profile "MobileFirst-byod_employee") #exit
```

```
(mm01) ^[aruba] (config) # ap-group CampusAP
```

Create the AP group and add
it to the virtual AP profile

```
(mm01) ^[aruba] (AP group "CampusAP") #virtual-ap MobileFirst-  
byod_employee
```

```
(mm01) ^[aruba] (AP group "CampusAP") #exit
```

```
(mm01) ^[aruba] (config) #write memory
```

HTTPS Server Certificate for MCs

Uploading a public HTTPS server certificate is more secure and provides an enhanced client onboarding experience for users connecting to SSIDs that utilize captive portal redirection. Clients should be redirected to webpages with certificates that are natively trusted. In the Aruba test network used for the Mobile First Base Designs Lab for ArubaOS 8, a public wildcard certificate *.aruba-tme.com is used on all Mobility Controllers. Using the public wildcard certificate improves the client onboarding experience in the employee and guest SSIDs since both utilize a captive portal.

Certificates can be uploaded using the following steps:

1. Log into the MM01 GUI
2. Select the hierarchy path **/Managed Network/aruba**
3. Navigate to **Configuration > System > Certificates**
4. Under Import Certificates, click the + button to bring up the New Certificate window
5. Browse to your certificate and fill in the fields
6. Click Submit to save.

The screenshot shows the Aruba GUI's 'Certificates' configuration page. At the top, there are navigation tabs: General, Admin, AirWave, CPsec, **Certificates**, SNMP, Logging, Profiles, and More. Below the tabs is a section titled 'Import Certificates' containing a table with the following data:

NAME	TYPE	FILENAME	REFERENCES	EXPIRED
master-ssh-pub-cert	PublicCert	master-ssh-pub-cert	--	--
STAR_aruba-tme_com	ServerCert	star_aruba-tme_com.pfx	--	--

Below the table is a '+' button, which is circled in red. A red line connects this button to a 'New Certificate' form, also outlined in red. The form contains the following fields:

- Certificate name: STAR_aruba-tme_com
- Certificate filename: star_aruba-tme_com.pfx (with a 'Browse' button next to it)
- Optional passphrase: [Redacted]
- Retype passphrase: [Redacted]
- Certificate format: DER (dropdown menu)
- Certificate type: CRL (dropdown menu)

At the bottom of the form are 'Export Certificates' and 'CSR' links, and 'Cancel' and 'Submit' buttons.

Figure 55 Uploading HTTPS Server Certificate via GUI

The certificate will be uploaded at this point to the four mobility controllers in the hierarchy. Use the following steps to assign the newly uploaded certificate to be used by the controller:

1. Select the hierarchy path **/Managed Network/aruba**
2. Navigate to **Configuration > System > Profiles > Other Profiles > Web Server Configuration**
 - Use the drop-down to select the newly uploaded certificate for Captive Portal
 - Optionally, use the same certificate for the switch
3. Click Submit to save and apply these changes to the four mobility controllers.

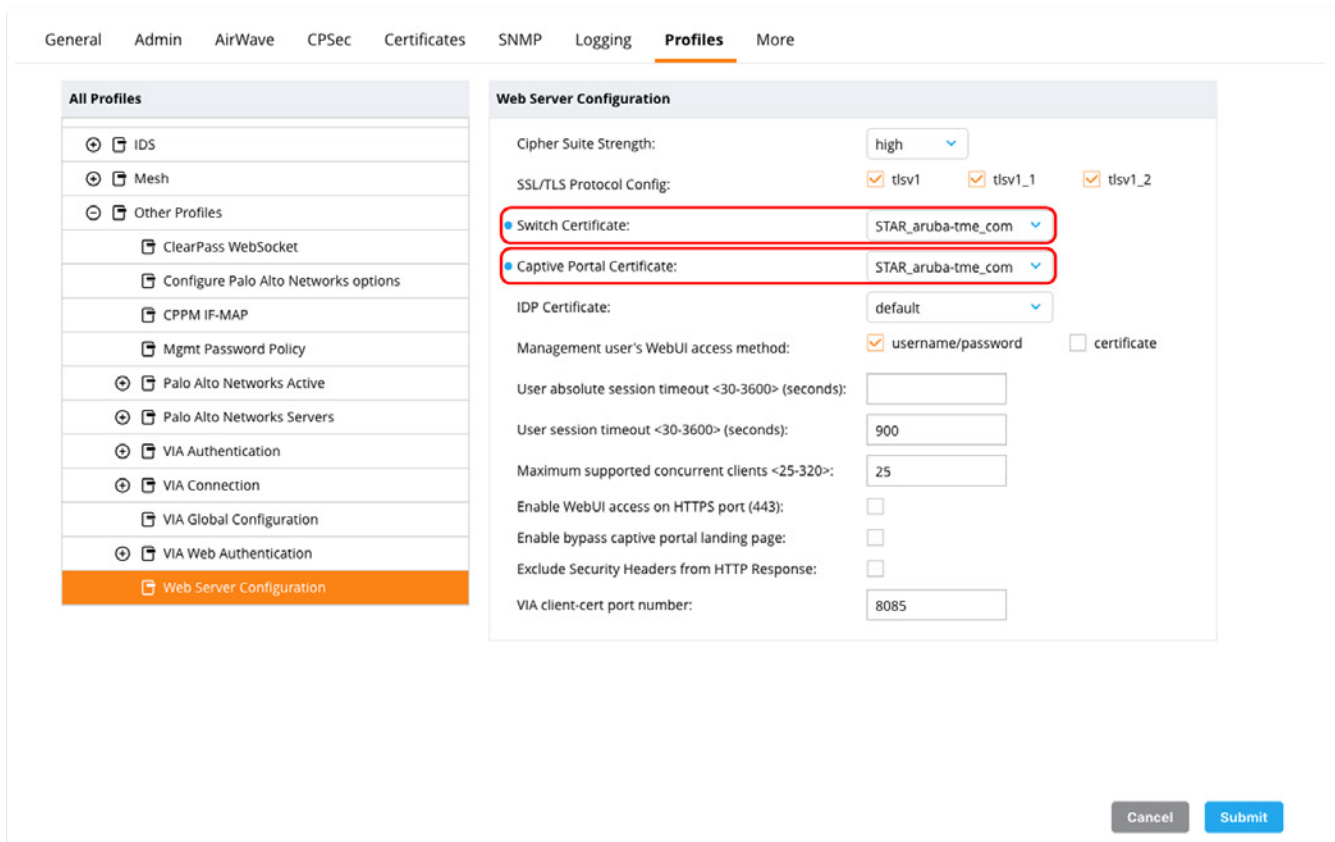


Figure 56 Assigning the Certificate to the Controller

BYOD Employee ClearPass Configuration

CP-Corp

Navigate to the address of CP-Corp in a web browser. Open ClearPass and log in. The default credentials for ClearPass are admin/eTIPS123.

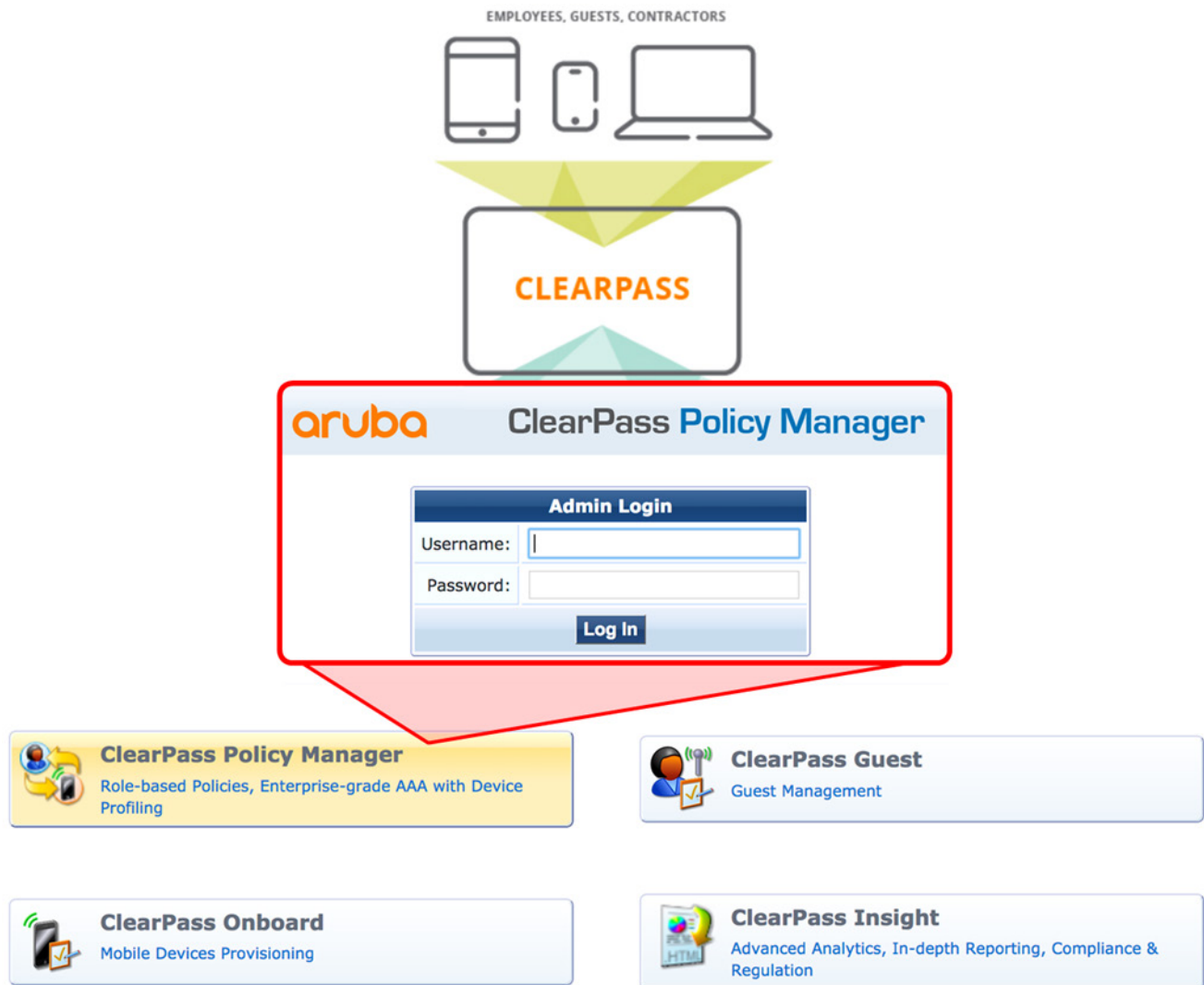


Figure 57 Log in to ClearPass

In the Mobile First Base Designs Lab for ArubaOS 8 test network CP-Corp is configured as seen in **Administration > Server Manager > Server Configuration > cp-corp**.

System		Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	<input type="text" value="cp-corp"/>					
FQDN:	<input type="text" value="cp-corp.aruba-tme.com"/>					
Policy Manager Zone:	<input type="text" value="default"/>					Manage Policy Manager Zones
Enable Profile:	<input checked="" type="checkbox"/> Enable this server for endpoint classification					
Enable Performance Monitoring Display:	<input checked="" type="checkbox"/> Enable this server for performance monitoring display					
Insight Setting:	<input type="checkbox"/> Enable Insight					
OnConnect Setting:	<input type="checkbox"/> Enable OnConnect					
Enable Ingress Events Processing:	<input type="checkbox"/> Enable Ingress Events processing on this server					
Span Port:	<input type="text" value="-- None --"/>					
		IPv4	IPv6	Action		
Management Port	IP Address	10.127.89.30		<input type="button" value="Configure"/>		
	Subnet Mask	255.255.255.0				
	Default Gateway	10.127.89.1				
Data/External Port	IP Address			<input type="button" value="Configure"/>		
	Subnet Mask					
	Default Gateway					
DNS Settings	Primary	10.127.3.11		<input type="button" value="Configure"/>		
	Secondary	10.127.3.12				
	Tertiary					
AD Domains:	Policy Manager is not part of any domain. Join to domain here.					<input type="button" value="Join AD Domain"/>
Back to Server Configuration						<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Figure 58 Adding CP-Corp to the AD Domain

The following steps need to be followed in order to add CP-Corp to AD Domain:

1. Click Join AD Domain
2. Enter the FQDN of the Domain Controller and Password, the example here assumes default admin user as Administrator. In this example, 'ad1.tmelab.net' is the domain controller (discoverable using the DNS server configured earlier). The NETBios name is automatically detected by ClearPass
3. Click **Save**. ClearPass will join the domain and show a status message.
4. Click **Close** at the bottom of the page and click **Save** again to exit *CP-Corp* configuration.

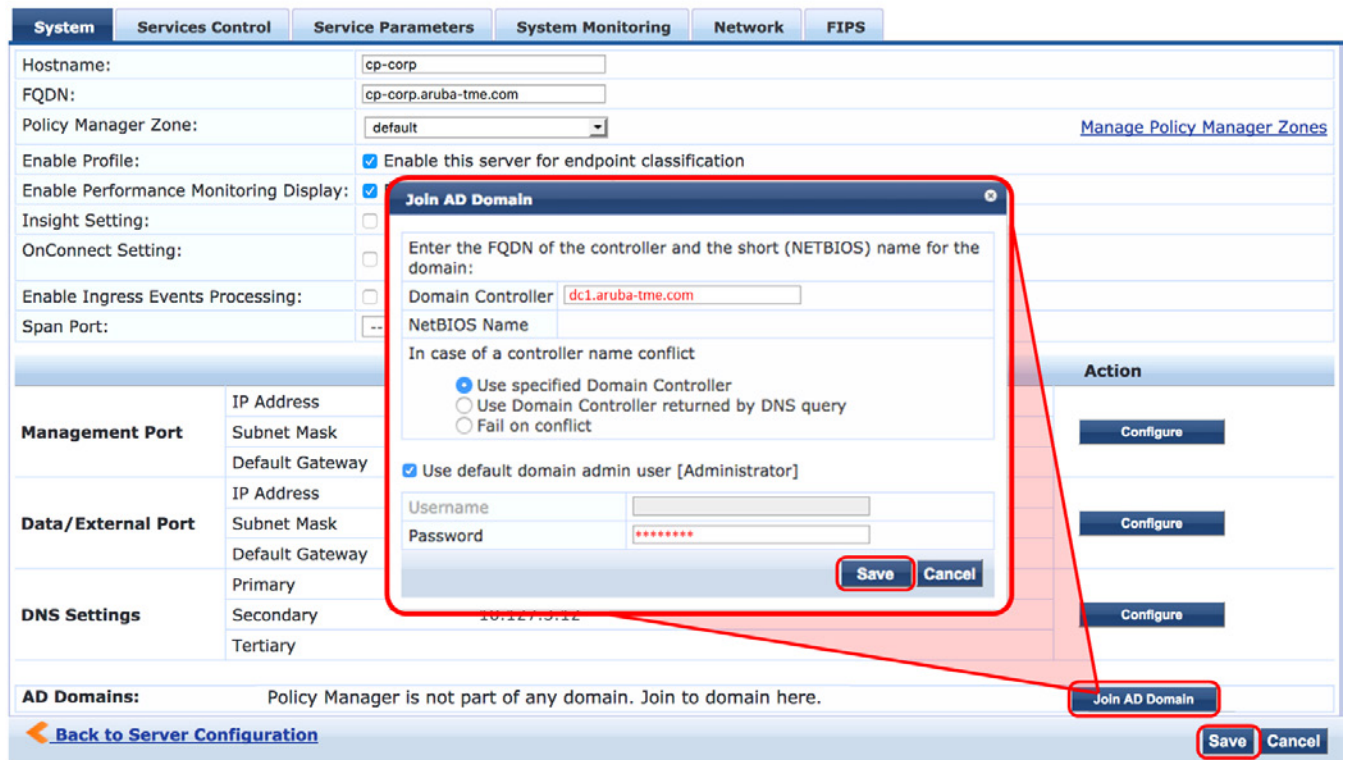


Figure 59 CP-Corp Added to the Domain

Trust List and Certificates

In order to upload the publicly signed HTTPS Server Certificate, the Trust List for the certificate must be added and enabled first.

1. Navigate to **Administration > Certificates > Trust List**
2. Click **Add**
3. In the pop-up window select the root CA certificate file and click **Add Certificate**
4. Repeat the steps above for any intermediate CA certificates applicable to your HTTPS Server Certificate

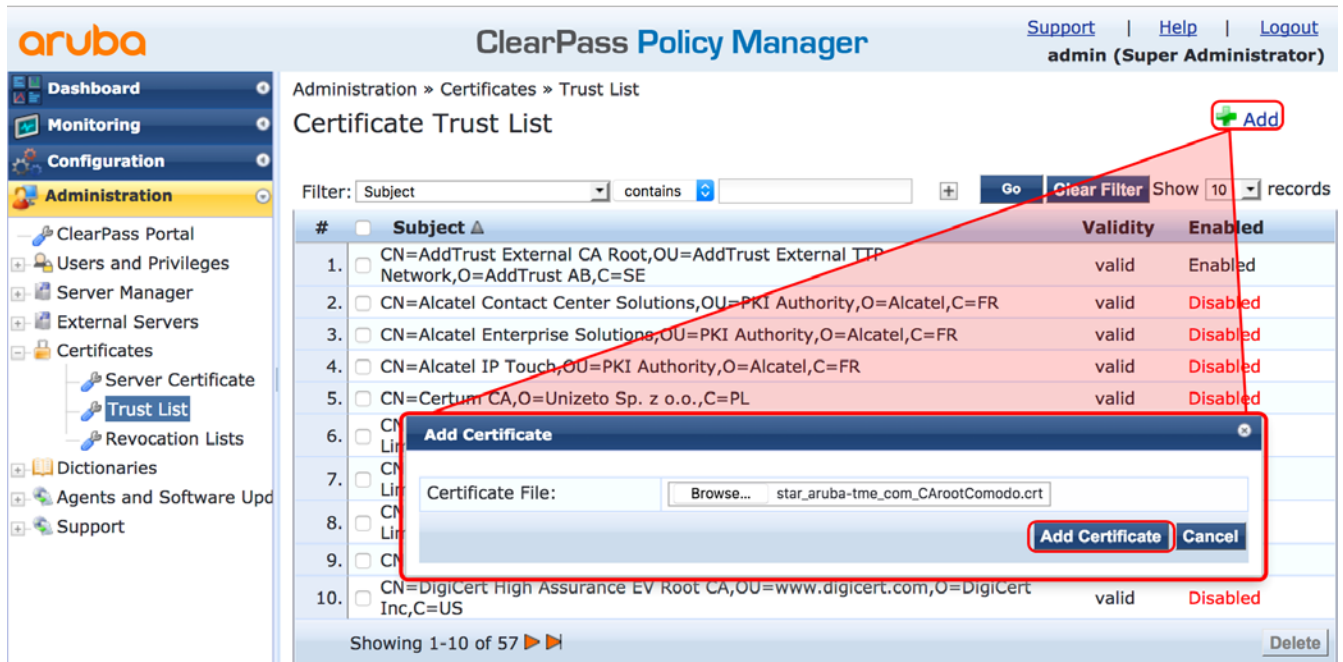
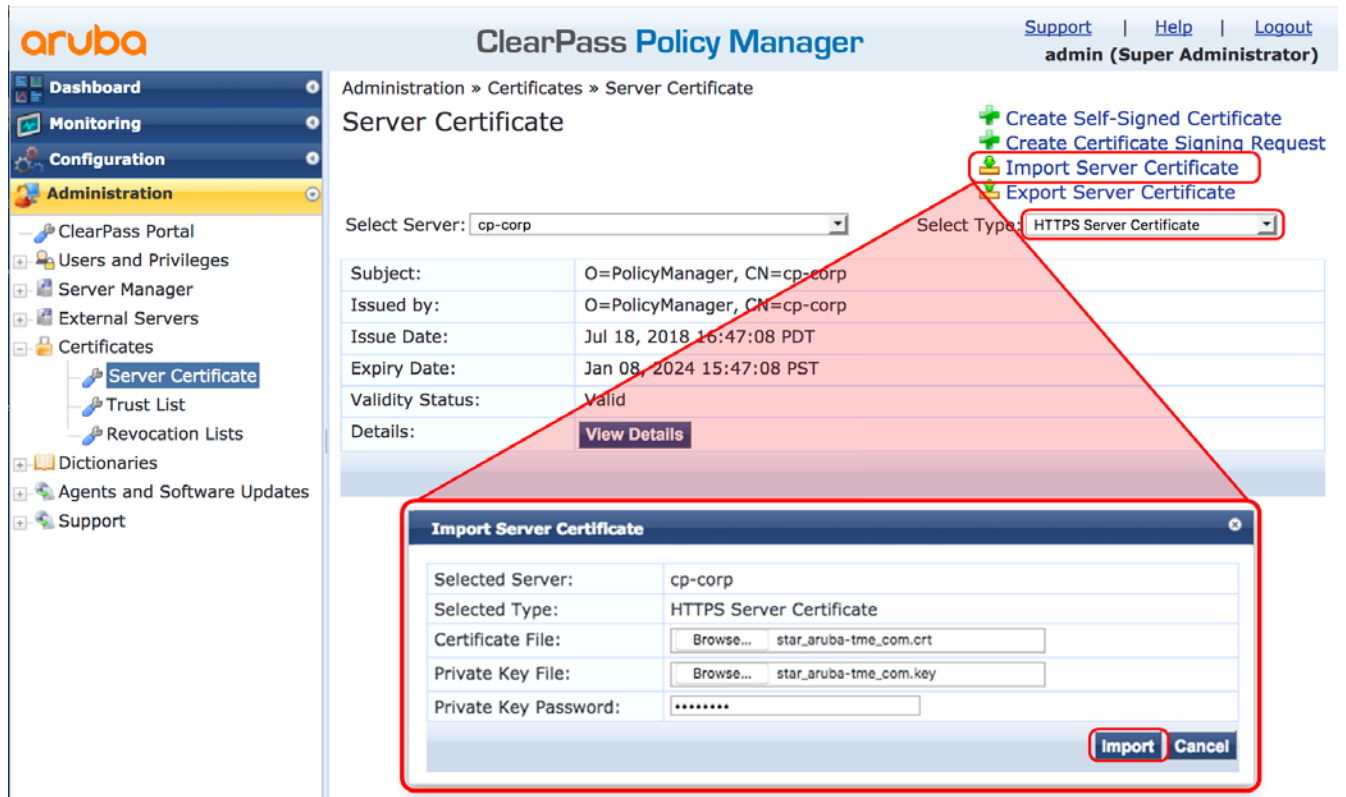


Figure 60 Add and Enable the Trust List

Next the Server Certificate must be uploaded. Errors will prevent the certificate from being imported if the Trust List requirement is not met first.

1. Navigate to **Administration > Certificates > Server Certificate**
2. Choose **HTTPS Server Certificate** under the **Select Type** dropdown
3. Click **Import Server Certificate**
4. Browse for the Certificate File
5. Brose for the Private Key File
6. Enter the Private Key Password
7. Click **Import**



Server Certificate updated successfully. Please log in again to continue...

Figure 61 *Uploading the Server Certificate*

Upon successful import, there will be a confirmation message. You will have to log out of ClearPass Policy Manager and log in again.

Network Devices

Navigate to **Configuration > Network > Devices**. Click **Add** in the top-right corner to add controllers to the list. Note that all 4 MCs have been added in a cluster using an IP range of 10.127.90.11-14.

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Network Devices' and shows a table of existing devices. A red box highlights the 'Add' button in the top right corner of the main content area. Below the table, the 'Add Device' dialog box is open, showing the following fields:

Attribute	Value
Name:	Mobility Controller Cluster
IP or Subnet Address:	10.127.90.11-14 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)
Description:	IPs for 4 mobility controllers in the campus cluster
RADIUS Shared Secret:	aruba123
TACACS+ Shared Secret:	
Vendor Name:	Aruba
Enable RADIUS CoA:	<input checked="" type="checkbox"/> RADIUS CoA Port: 3799

The 'Add' button is highlighted with a red box.

Figure 62 Adding Corp Controllers as Devices to ClearPass

The VIP addresses for all 4 controllers in the campus cluster must also be added for CoA.

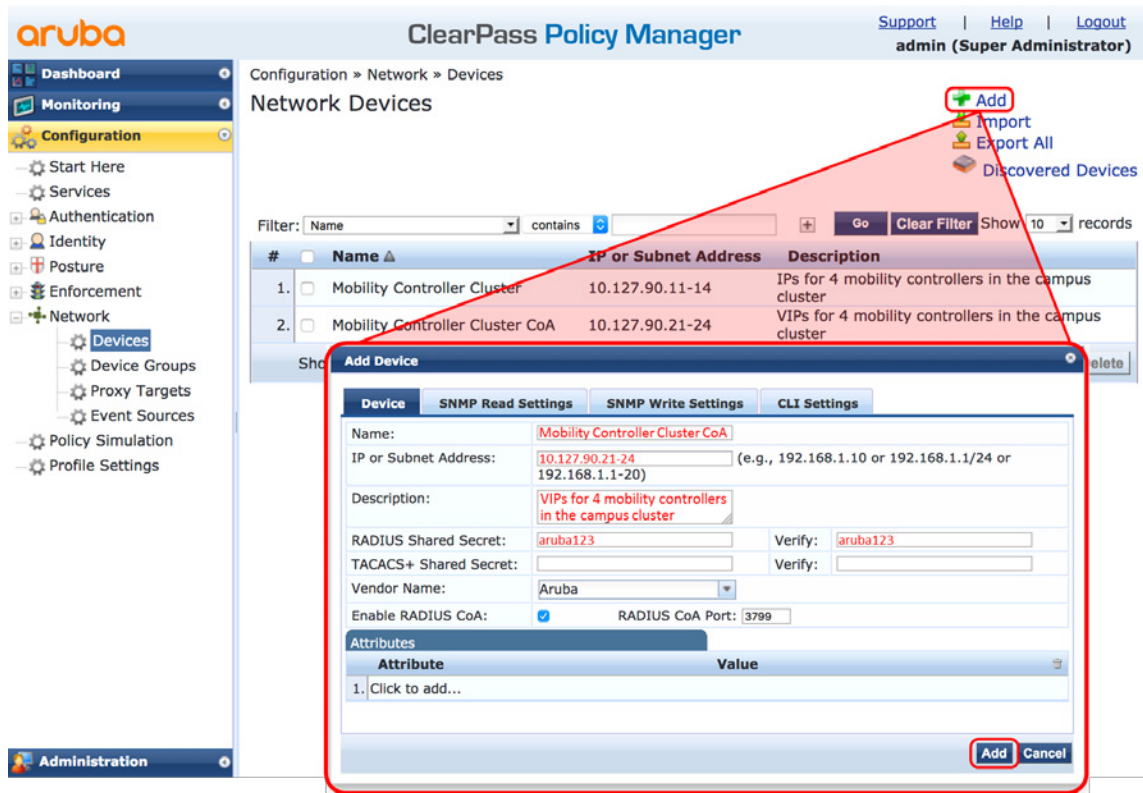


Figure 63 Adding the VIPs for the Controllers in the Campus Cluster

Authentication Methods

Two authentication methods will be added: byod_employee EAP-TLS and byod_employee EAP-PEAP. Navigate to **Configuration > Authentication > Methods** and click **Add**.

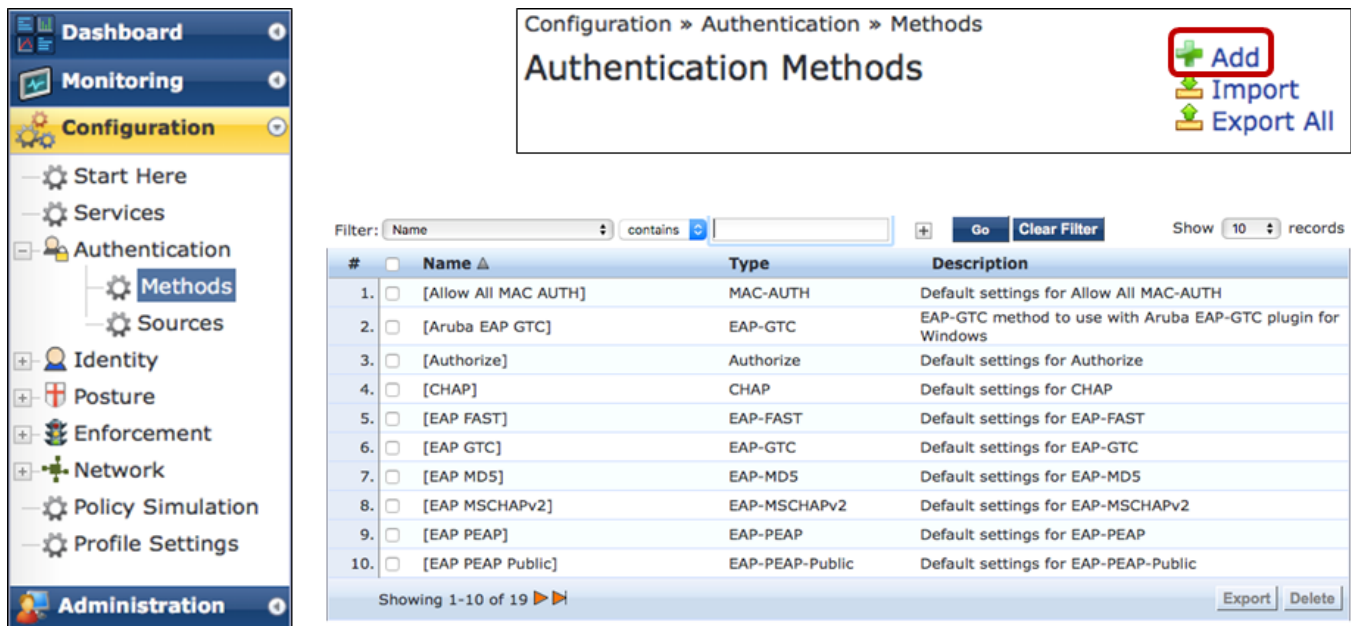


Figure 64 Add Authentication Method

Enter the details for byod_employee EAP-TLS and click **Save** when finished. Note that the **Session Resumption** box needs to be left unchecked so as to disable the feature.

The screenshot shows the 'Add Authentication Method' dialog box with the 'General' tab selected. The 'Name' field is 'byod_employee EAP-TLS' and the 'Description' is 'Auth method for byod_employee WLAN'. The 'Type' dropdown is set to 'EAP-TLS'. In the 'Method Details' section, 'Session Resumption' is unchecked, 'Session Timeout' is 6 hours, 'Authorization Required' is checked, 'Certificate Comparison' is 'Do not compare', 'Verify Certificate using OCSP' is 'None', and 'Override OCSP URL from Client' is unchecked. The 'OCSP URL' field is empty. 'Save' and 'Cancel' buttons are at the bottom right.

Figure 65 Adding the byod_employee EAP-TLS Authentication Method

Enter the details for byod_employee EAP-PEAP and click **Save** when finished.

*The same popup window, different tabs.

The left screenshot shows the 'Add Authentication Method' dialog box with the 'General' tab selected. The 'Name' field is 'byod_employee EAP-PEAP' and the 'Description' is 'Auth method for byod_employee WLAN'. The 'Type' dropdown is set to 'EAP-PEAP'. In the 'Method Details' section, 'Session Resumption' is checked, 'Session Timeout' is 6 hours, 'Fast Reconnect' is checked, 'Microsoft NAP Support' is unchecked, and 'Cryptobinding' is 'None'. The 'Save' and 'Cancel' buttons are at the bottom right.

The right screenshot shows the 'Add Authentication Method' dialog box with the 'Inner Methods' tab selected. The 'Specify inner Authentication Methods in the preferred order:' section contains a list with '[EAP MSCHAPv2](Default)'. Below the list is a dropdown menu with '--Select a method--'. To the right of the list are 'Default' and 'Remove' buttons. A note says '**To add this field, use the drop-down box below.' and another note says 'To set preference for a specific method, use Default button'. The 'Save' and 'Cancel' buttons are at the bottom right.

Figure 66 Adding the byod_employee EAP-PEAP Authentication Method

Verify the added authentication methods on the **Configuration > Authentication > Methods** page.

Configuration » Authentication » Methods

Authentication Methods

[Add](#)
[Import](#)
[Export All](#)

Filter: Name contains Go Clear Filter Show 10 records

#	Name	Type	Description
1.	[Allow All MAC AUTH]	MAC-AUTH	Default settings for Allow All MAC-AUTH
2.	[Aruba EAP GTC]	EAP-GTC	EAP-GTC method to use with Aruba EAP-GTC plugin for Windows
3.	[Authorize]	Authorize	Default settings for Authorize
4.	byod_employee EAP-PEAP	EAP-PEAP	Auth method for byod_employee WLAN
5.	byod_employee EAP-TLS	EAP-TLS	Auth method for byod_employee WLAN
6.	[CHAP]	CHAP	Default settings for CHAP
7.	[EAP FAST]	EAP-FAST	Default settings for EAP-FAST
8.	[EAP GTC]	EAP-GTC	Default settings for EAP-GTC
9.	[EAP MD5]	EAP-MD5	Default settings for EAP-MD5
10.	[EAP MSCHAPv2]	EAP-MSCHAPv2	Default settings for EAP-MSCHAPv2

Showing 1-10 of 22 Export Delete

These authentication methods were just added.

Figure 67 Summary of Authentication Methods

Authentication Sources

The Active Directory must be added as an authentication source. Navigate to **Configuration > Authentication > Sources** and click **Add**.

Configuration » Authentication » Sources

Authentication Sources

[Add](#)
[Import](#)
[Export All](#)

Filter: Name contains Go Clear Filter Show 10 records

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
3.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
8.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
9.	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database
10.	[Time Source]	Local SQL DB	Authorization source for implementing various time functions

Showing 1-10 of 10 Copy Export Delete

Figure 68 Add Authentication Sources

1. In the **General** tab, enter the Name, Description, and Type for the Active Directory
2. Click **Next**

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary Attributes Summary

Name: Corporate AD

Description: Active Directory for corporate users

Type: Active Directory

Use for Authorization: Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources:

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority:

Back to Authentication Sources Next > Save Cancel

Figure 69 Enter Corporate AD Details – General Tab

3. Enter the connection details for the active directory
4. Click **Save**



Note: You will need to know the login credentials for the network's domain controller.

Configuration » Authentication » Sources » Add - Corporate AD

Authentication Sources - Corporate AD

Summary **Primary** Attributes Backup 1

Connection Details

Hostname: dc1.aruba-tme.com

Connection Security: None

Port: 389 (For secure connection, use 636)

Verify Server Certificate: Enable to verify Server Certificate for secure connection

Bind DN: administrator@aruba-tme.com
(e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)

Bind Password: *****

NetBIOS Domain Name: ARUBA-TME

Base DN: dc=aruba-tme,dc=com [Search Base Dn](#)

Search Scope: SubTree Search

LDAP Referrals: Follow referrals

Bind User: Allow bind using user password

User Certificate : userCertificate

Always use NETBIOS name: Enable to always use NETBIOS name instead of the domain part in username for authentication

Back to Authentication Sources Clear Cache Copy Save Cancel

Figure 70 Enter Corporate AD Details - Primary Tab

Navigate to **Configuration > Authentication > Sources** to verify the authentication source.

Configuration » Authentication » Sources

Authentication Sources

[Add](#)
[Import](#)
[Export All](#)

This source has just been added.

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
3.	Corporate AD	Active Directory	Active Directory of corporate users.
4.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
5.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
6.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
7.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
8.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
9.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
10.	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database

Showing 1-10 of 11

[Copy](#) [Export](#) [Delete](#)

Figure 71 Summary of Authentication Sources

Service Templates

Navigate to **Configuration > Start Here**. Scroll to the bottom and click **Onboard**.

aruba ClearPass Policy Manager

Support | Help | Logout
admin (Super Administrator)

Guest Social Media Authentication

To authenticate guest users logging in via captive portal with their social media accounts. Guests must re-authenticate after their session ends.

OAuth2 API User Access

Service template for API clients authenticating with username and password (OAuth2 grant type "password")

Onboard

Service template for authorizing device credential provisioning and onboarding.

Figure 72 Start Onboard Service Templates

The following screen opens:

Service Templates - Onboard

General | **Wireless Network Settings** | Device Access Restrictions | Provisioning Wireless Network Settings

Select Prefix:

Name Prefix*:

Description

Create an Onboard Pre-Auth service to check the user's credentials prior to starting the device provisioning process. Create an authorization service that checks whether a user's device may be provisioned using Onboard. Use an Aruba 802.1X wireless service to authenticate users prior to device provisioning with Onboard, and also after device provisioning is complete.

[Back to Start Here](#)

Figure 73 Onboard Service Templates - General Tab

1. Enter a Name Prefix for the WLAN
2. Click **Next**

Service Templates - Onboard

General | **Wireless Network Settings** | Device Access Restrictions | Provisioning Wireless Network Settings

Select a wireless controller from the list, or create a new one

Select Wireless Controller:

Wireless Controller Name:

Controller IP Address:

Vendor Name:

RADIUS Shared Secret:

Enable RADIUS CoA:

RADIUS CoA Port:

[Back to Start Here](#)

Figure 74 Onboard Service Templates - Wireless Network Settings Tab

3. Select a wireless controller. The choices will be the devices that were configured at the beginning of this section
4. Click **Next**

Service Templates - Onboard

General | Wireless Network Settings | **Device Access Restrictions** | Provisioning Wireless Network Settings

Enable the days on which onboarded devices are allowed network access

Days allowed for access*: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

[Back to Start Here](#)

Figure 75 Onboard Service Templates - Device Access Restrictions Tab

5. Leave this tab as default
6. Click **Next**

Service Templates - Onboard

General | Wireless Network Settings | Device Access Restrictions | **Provisioning Wireless Network Settings**

Provisioning Settings

Wireless SSID for Onboard Provisioning*: [Add new Onboard Network settings](#)

[Back to Start Here](#)

Figure 76 Onboard Service Templates - Provisioning Wireless Network Settings Tab

7. Enter the SSID
8. Click **Add Service**

When the Onboard Service Templates is complete, a summary of added content appears:

- **Added 3 Enforcement Profile(s)**
- **Added 3 Enforcement Policies**
- **Added 1 Role Mapping Policies**
- **Added 3 service(s)**

Figure 77 Onboard Service Templates Summary

Enforcement Profiles

The content that was added by the Service Template must be edited. Three new enforcement profiles now exist in **Configuration > Enforcement > Profiles**, two of which may need to be adjusted.

The Onboard Post-Provisioning profile and Onboard Pre-Provisioning Profile should be edited. Proceed to edit by clicking on the profile name.

#	Name	Type	Description
1.	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
3.	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
4.	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
5.	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
6.	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
7.	[Aruba Bounce Host-Port]	RADIUS_CoA	System-defined profile to bounce host-port (Aruba)
8.	[Aruba TACACS read-only Access]	TACACS	System-defined profile for read-only access to Aruba device
9.	[Aruba TACACS root Access]	TACACS	System-defined profile for root access to Aruba device
10.	[Aruba Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aruba)
11.	byod_employee Onboard Post-Provisioning	RADIUS	
12.	byod_employee Onboard Pre-Provisioning	RADIUS	
13.	byod_employee Onboard Session Timeout	Application	

Figure 78 Editing Enforcement Profiles

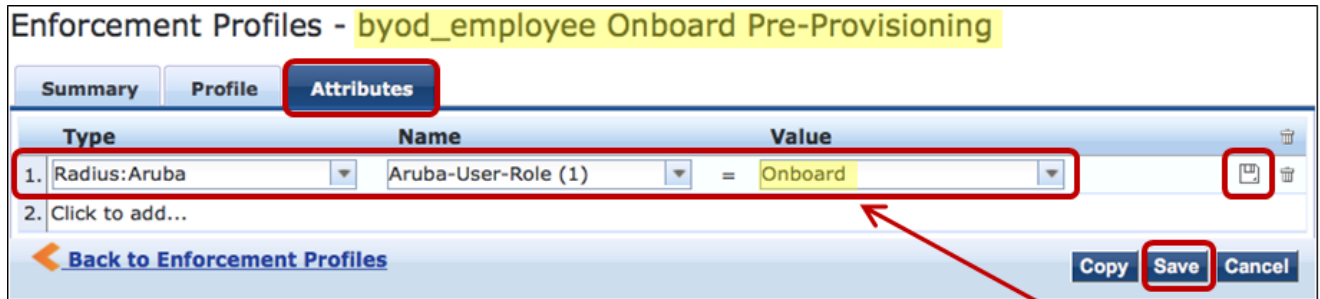
1. Ensure that the value field in the Onboard Post-Provisioning profile is an exact match for the name of the user role that was configured on the controllers
2. Click **Save** when done

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role (1)	= mobilefirst-byod_employee
2. Click to add...		

This value must match the user-role name on the mobility controllers.

Figure 79 Editing the Onboard Post-Provisioning Profile

3. Ensure that the value field in the Onboard Pre-Provisioning profile is an exact match for the name of the user-role that was configured on the controllers
4. Click **Save** when done



This value must match user-role name on the controller.

Figure 80 Editing the Onboard Pre-Provisioning Profile

Enforcement Policies

Once the profiles have been properly configured it is time to edit the enforcement policies. The content that the Service Template added must be edited. Two new enforcement profiles now exist in **Configuration > Enforcement > Policies**:

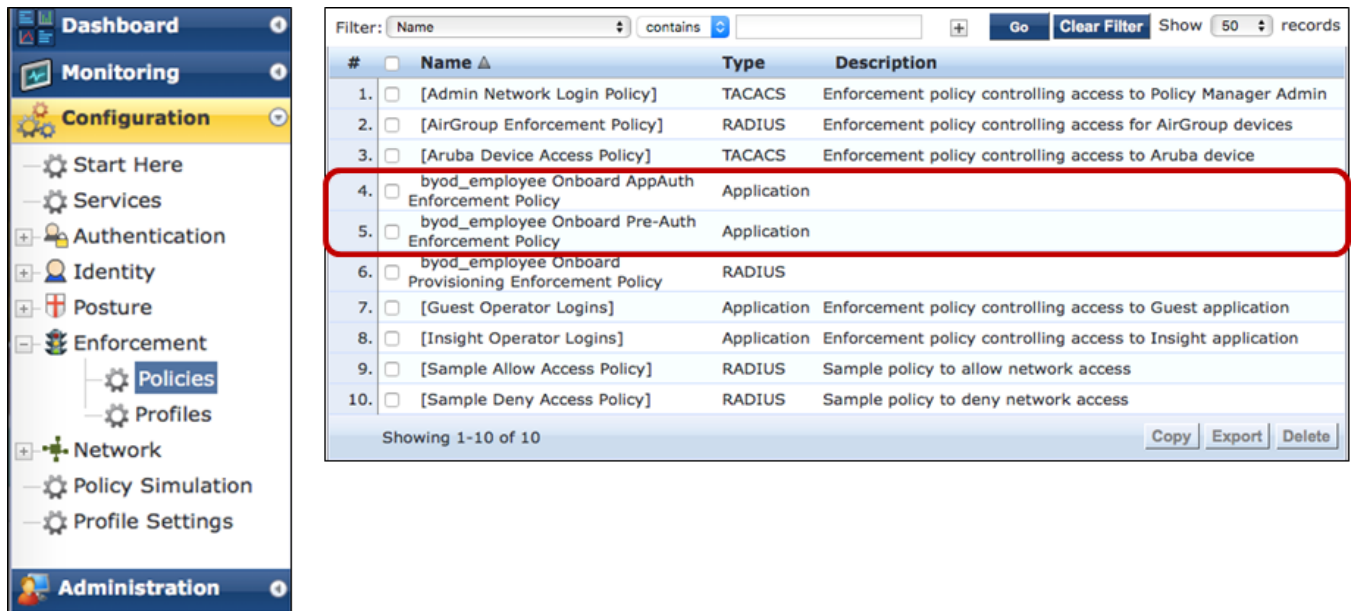


Figure 81 Editing Enforcement Policies

A few adjustments will need to be made. Click the name of a policy to begin editing.

1. Remove the first rule In the Onboard AppAuth Enforcement Policy
2. Click **Save**

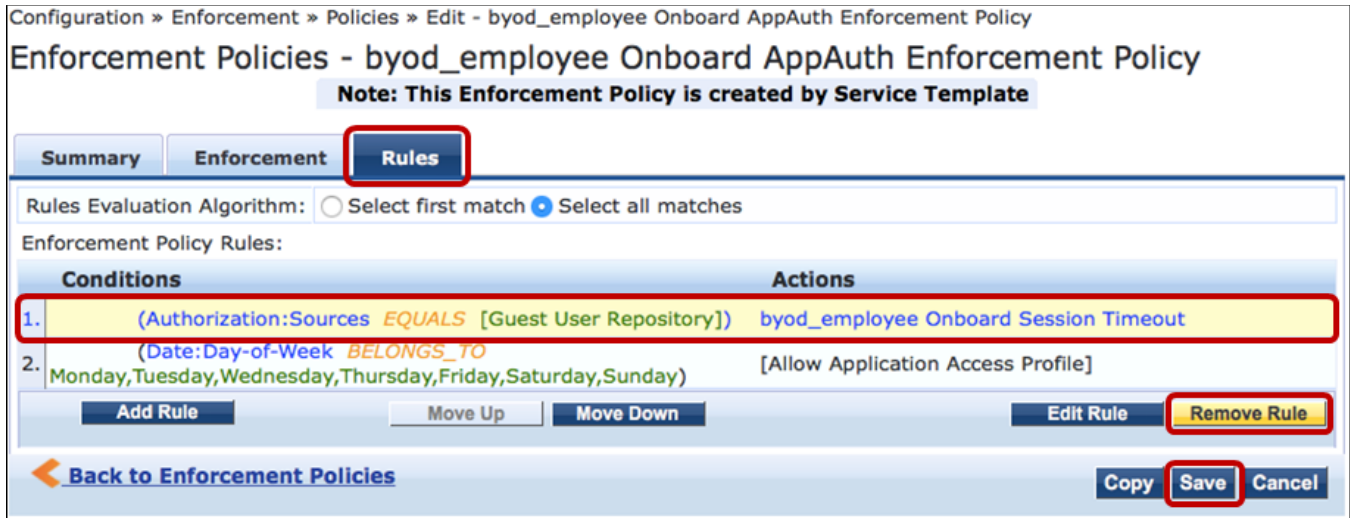


Figure 82 Editing the AppAuth Enforcement Policy

3. Access is allowed for every day of the week In the Onboard Pre-Auth Enforcement Policy. This policy does not need to be edited
4. Click **Cancel** to leave the screen

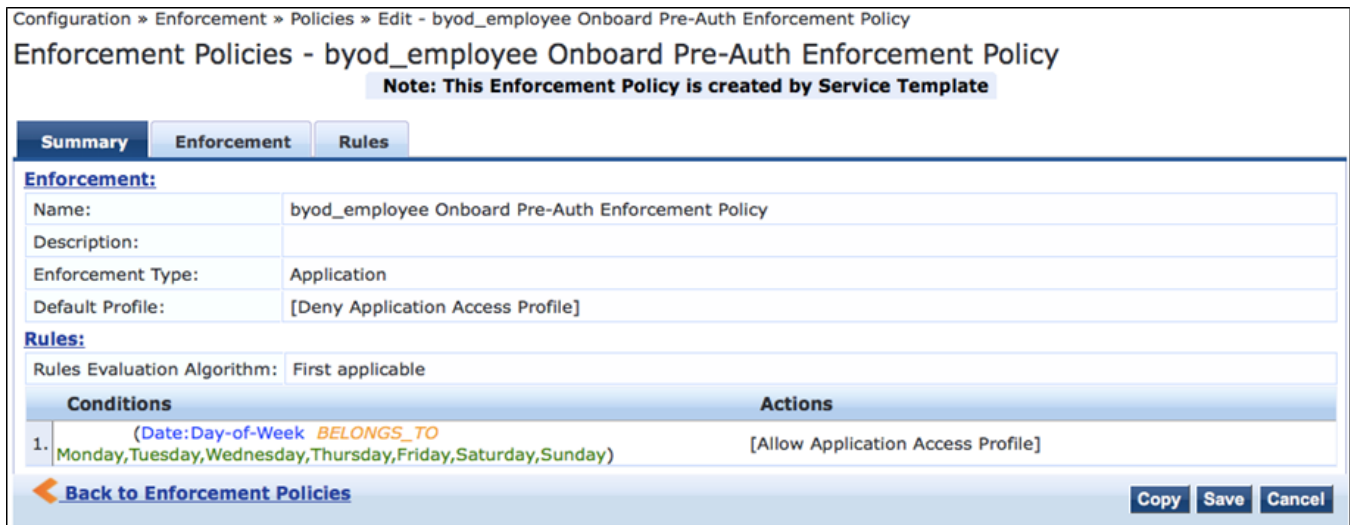


Figure 83 Editing the Pre-Auth Enforcement Policy

Services

Three services were added in **Configuration > Services**. Authentication methods and sources must be adjusted in each of the newly added services. Click the name of a service to begin editing.

The screenshot shows the ArubaOS configuration interface. On the left is a navigation menu with sections: Dashboard, Monitoring, Configuration, and Administration. Under Configuration, there are sub-items: Start Here, Services, Authentication, Identity, Posture, Enforcement, Network, Policy Simulation, and Profile Settings. The main area displays the 'Configuration > Services' page. At the top right are buttons for 'Add', 'Import', and 'Export All'. Below is a filter bar with 'Name' and 'contains' dropdowns, and 'Go' and 'Clear Filter' buttons. A 'Show 50 records' dropdown is also present. The main content is a table with columns: #, Order, Name, Type, Template, and Status. The table lists 8 services. The 6th, 7th, and 8th services are highlighted with a red box:

#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
3.	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	●
4.	4	[Guest Operator Logins]	Application	Aruba Application Authentication	●
5.	5	[Insight Operator Logins]	Application	Aruba Application Authentication	●
6.	6	byod_employee Onboard Provisioning	RADIUS	Aruba 802.1X Wireless	●
7.	7	byod_employee Onboard Authorization	Application	Aruba Application Authentication	●
8.	8	byod_employee Onboard Pre-Auth	Application	Aruba Application Authentication	●

At the bottom of the table, it says 'Showing 1-8 of 8' and there are buttons for 'Reorder', 'Copy', 'Export', and 'Delete'.

Figure 84 Editing Services

Click **Onboard Pre-Auth** to edit that service.

1. Add the Corporate AD source created in the [Authentication Sources](#) section
2. Click **Save**

The screenshot shows the 'Configuration > Services > Edit - byod_employee Onboard Pre-Auth' page. The title is 'Services - byod_employee Onboard Pre-Auth' with a note: 'Note: This Service is created by Service Template'. There are tabs for 'Summary', 'Service', 'Authentication', 'Roles', and 'Enforcement'. The 'Authentication' tab is selected and highlighted with a red box. Under 'Authentication Sources', there is a list containing 'Corporate AD [Active Directory]', which is also highlighted with a red box. To the right of the list are buttons: 'Move Up', 'Move Down', 'Remove', 'View Details', and 'Modify'. Below the list is a dropdown menu with '--Select to Add--'. At the bottom, there is a checkbox for 'Strip Username Rules' with the text 'Enable to specify a comma-separated list of rules to strip username prefixes or suffixes'. At the bottom right are buttons: 'Enable', 'Copy', 'Save', and 'Cancel'. The 'Save' button is highlighted with a red box.

Figure 85 Editing the Onboard Pre-Auth Service

The **Summary** tab shows an overview of the Onboard Pre-Auth service.

Configuration » Services » Edit - byod_employee Onboard Pre-Auth

Services - byod_employee Onboard Pre-Auth

Note: This Service is created by Service Template

Summary Service Authentication Roles Enforcement

Service:

Name: byod_employee Onboard Pre-Auth

Description:

Type: Aruba Application Authentication

Status: Enabled

Monitor Mode: Disabled

More Options: -

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Application	Name	EQUALS	Onboard
2.	Application:ClearPass	Device-Name	NOT_EXISTS	

Authentication:

Authentication Sources: Corporate AD

Strip Username Rules: -

Roles:

Role Mapping Policy: [Guest Roles]

Enforcement:

Use Cached Results: Disabled

Enforcement Policy: byod_employee Onboard Pre-Auth Enforcement Policy

[Back to Services](#) Disable Copy Save Cancel

Figure 86 Summary of Onboard Pre-Auth Service

From the **Configuration > Services** menu select **byod_employee Onboard Authorization**.

1. Add the Corporate AD source created in the [Authentication Sources](#) section
2. Click **Save**

Configuration » Services » Edit - byod_employee Onboard Authorization

Services - byod_employee Onboard Authorization

Note: This Service is created by Service Template

Summary Service **Authorization** Roles Enforcement

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Authorization Details: Additional authorization sources from which to fetch role-mapping attributes -

Corporate AD [Active Directory] Remove View Details Modify [Add new Authentication Source](#)

--Select to Add--

[Back to Services](#) Enable Copy **Save** Cancel

Figure 87 Editing the Onboard Authorization Service

The **Summary** tab shows an overview of the Onboard Authorization service.

Configuration » Services » Edit - byod_employee Onboard Authorization

Services - byod_employee Onboard Authorization

Note: This Service is created by Service Template

Summary Service Authorization Roles Enforcement

Service:

Name:	byod_employee Onboard Authorization
Description:	Onboard Authorization Service for Applications
Type:	Aruba Application Authorization
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Application	Name	EQUALS	Onboard
2.	Application:ClearPass	Device-Name	EXISTS	

Authorization:

Strip Username Rules:	-
Authorization Details:	Corporate AD

Roles:

Role Mapping Policy:	byod_employee Onboard AppAuth Role Mapping
----------------------	--

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	byod_employee Onboard AppAuth Enforcement Policy

[Back to Services](#) Disable Copy Save Cancel

Figure 88 Summary of Onboard Authorization Service

Click **Onboard Provisioning** to edit that service.

1. Add the authentication methods created in the [Authentication Methods](#) section
2. Add the Corporate AD source created in the [Authentication Sources](#) section
3. Click **Save**

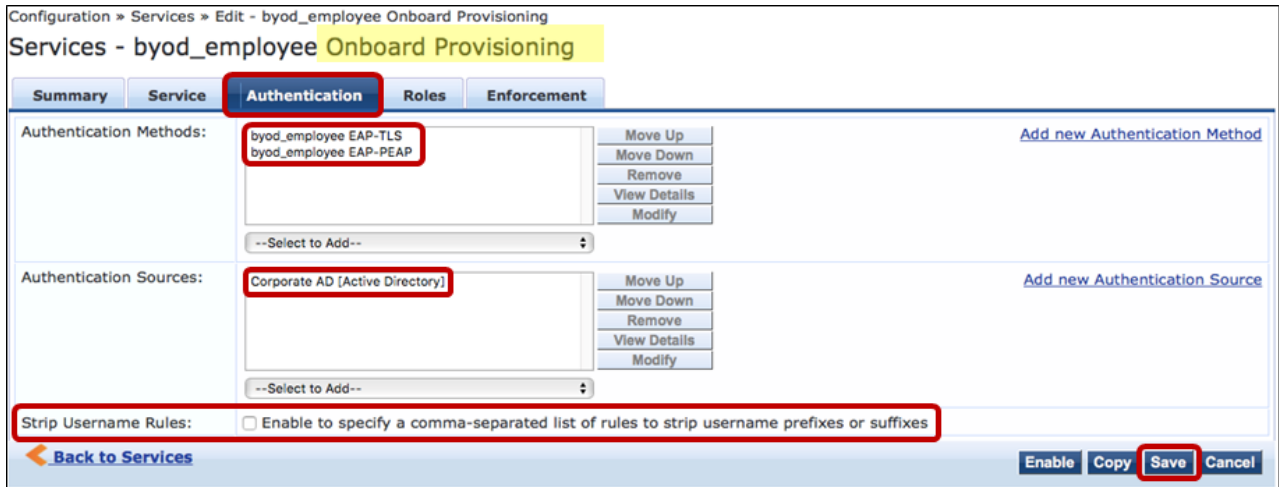


Figure 89 Editing the Onboard Provisioning Service

The **Summary** tab for the Onboard Provisioning service shows an overview.

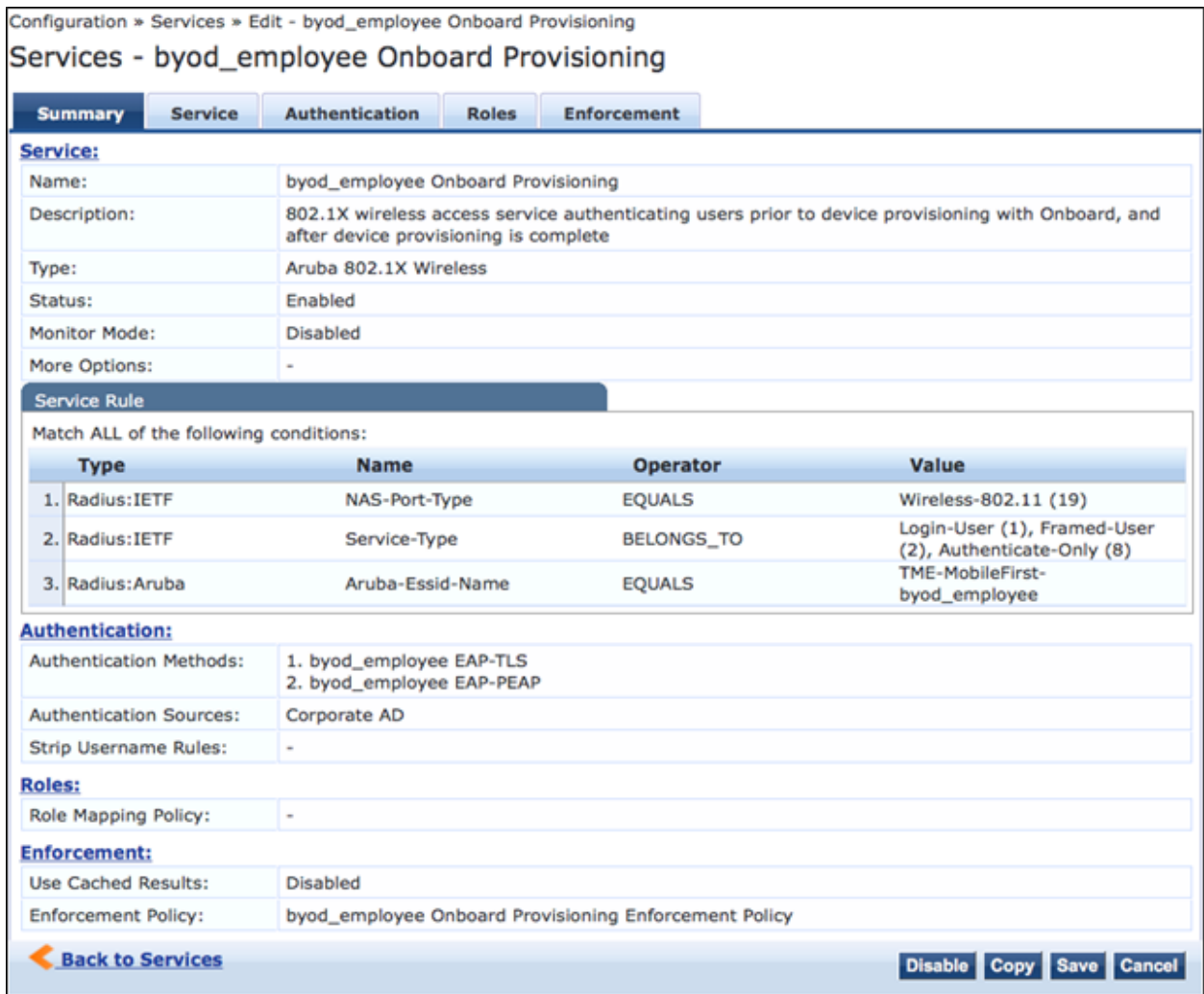


Figure 90 Summary of the Onboard Provisioning Service

BYOD Employee Onboard Configuration

The onboarding service requires configuration of a certificate authority (CA), network settings, a configuration profile, and provisioning settings. Navigate to the ClearPass Web page and login to the Onboard section.

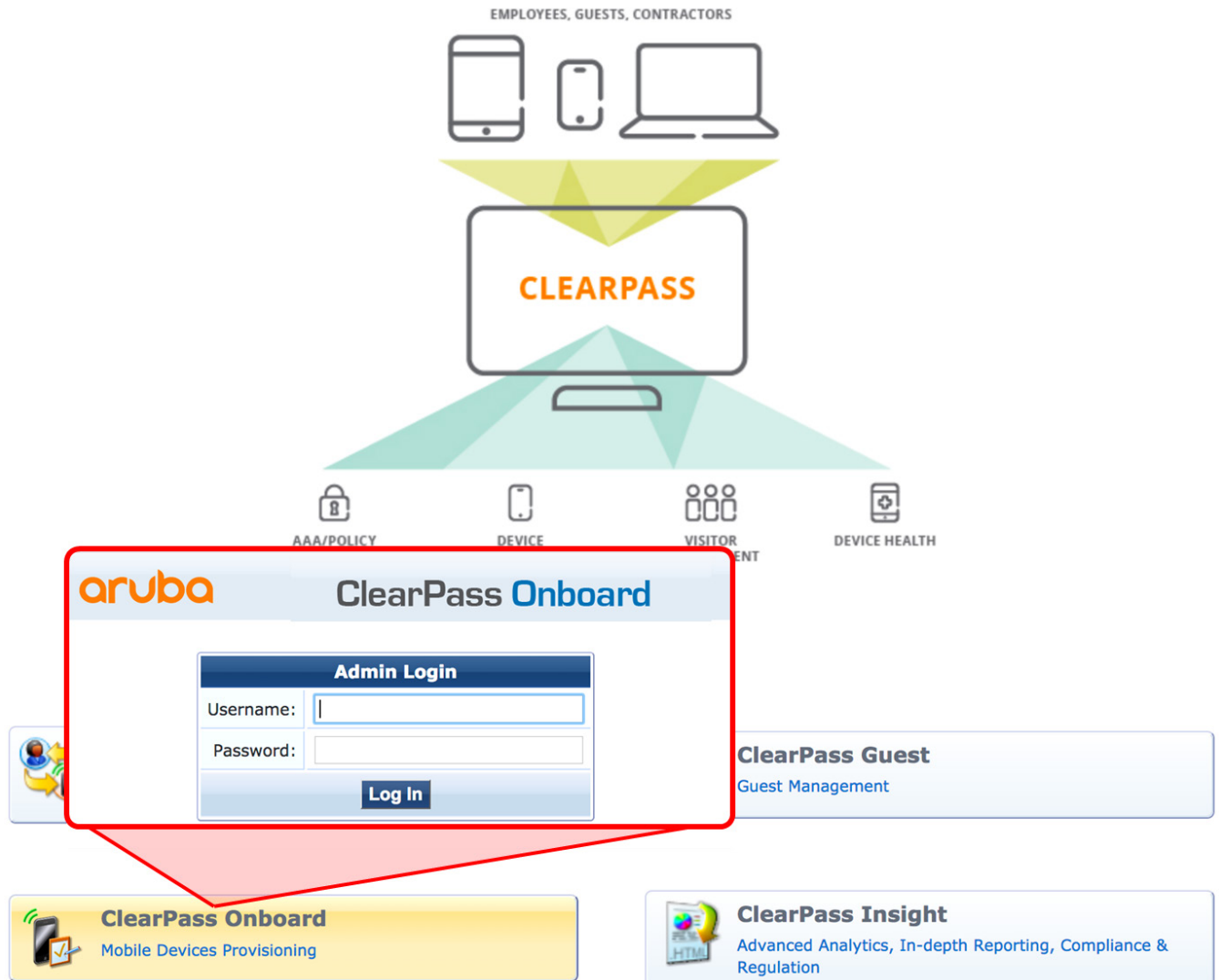


Figure 91 Log In to ClearPass Onboard

Certificate Authority

In the left-side pane, navigate to **Onboard > Certificate Authorities**.

1. Click **Create new certificate authority**
2. Enter the following details:
 - Name: byod_employee Certificate Authority
 - Mode: Root CA
 - Everything else can be left as default
3. Click **Create Certificate Authority** at the bottom of this page

The screenshot shows the Aruba Onboard web interface. On the left is a navigation pane with a tree view. The 'Onboard' section is expanded, and 'Certificate Authorities' is selected. The main content area is titled 'Certificate Authorities' and contains a 'Create new certificate authority' button at the top right. Below this is the 'Certificate Authority Settings' form. The 'Name' field is filled with 'byod_employee Certificate Authority'. The 'Description' field is empty. Below the description is a diagram of a 'Root CA' with a self-signed root certificate and client certificates. At the bottom of the form is a 'Create Certificate Authority' button.

Figure 92 *Creating the Certificate Authority*

Network Settings

In the left-side pane navigate to **Onboard > Configuration > Network Settings**.

1. Click **Create new network**

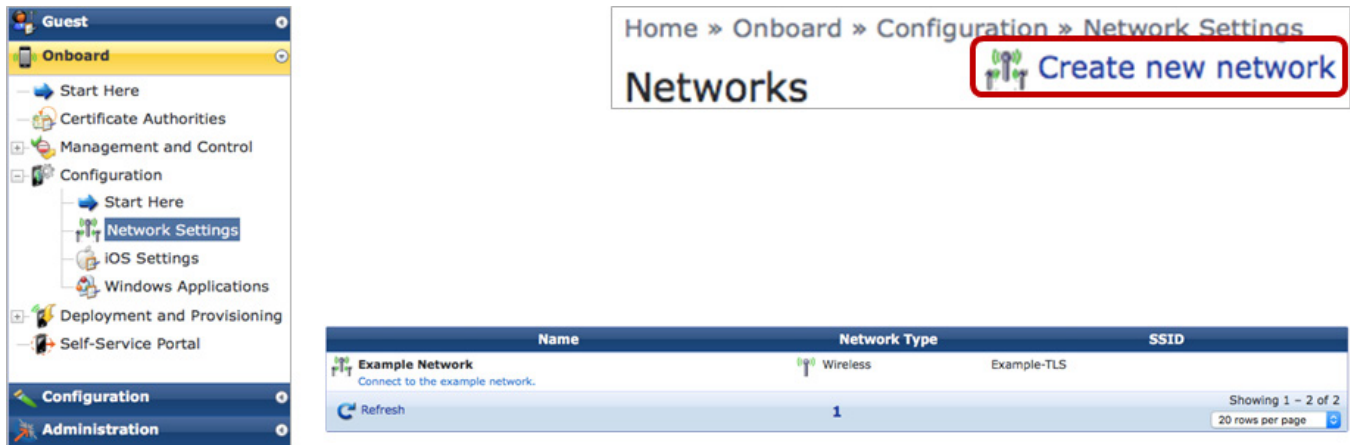


Figure 93 *Creating the Network Settings*

2. Enter the following details:
 - Name: byod_employee Network Settings
 - SSID: TME-MobileFirst-byod_employee
 - Everything else can be left as default
3. Click **Save Changes**

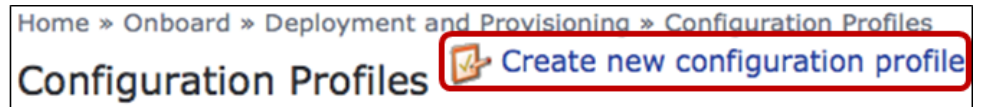
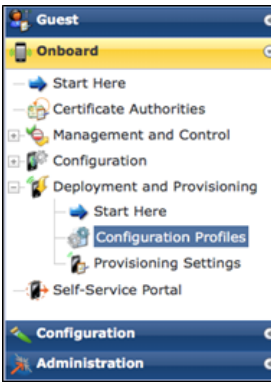
Network Settings » Network Access	
<p> Access Protocols Authentication Trust Windows Proxy </p>	
<h3>Network Access</h3> <p>Options for basic network access.</p>	
* Name:	<input type="text" value="byod_employee Network Settings"/> <p>Enter a name for the network.</p>
Description:	<div style="border: 1px solid #ccc; height: 60px;"></div> <p>Enter a description for the network.</p>
* Network Type:	<input type="text" value="Wireless only"/> <p>Select which types of network will be provisioned. Enterprise security (802.1X) will be selected if wired networks are to be supported.</p>
* Security Type:	<input type="text" value="Enterprise (802.1X)"/> <p>Select the authentication method used for the network. Enterprise security (802.1X) will be selected if wired networks are to be supported.</p>
<h3>Wireless Network Settings</h3> <p>Options for wireless network access.</p>	
* Security Version:	<input type="text" value="WPA2 with AES (recommended)"/> <p>Select the WPA encryption version for the wireless network. This setting is used for Windows, Android and Legacy OS X (10.5/6) devices only. iOS and OS X 10.7+ (Lion or later) devices auto-detect the WPA version.</p>
* SSID:	<input type="text" value="TME-MobileFirst-byod_employee"/> <p>Enter the SSID of the wireless network to connect to.</p>
Wireless:	<input type="checkbox"/> Hidden network Select this option if the wireless network is not open or broadcasting.
Auto Join:	<input checked="" type="checkbox"/> Automatically join network Select this option to automatically join the wireless network.
<p> <input type="button" value="Next"/> <input type="button" value="Save Changes"/> <input type="button" value="Cancel"/> </p>	

Figure 94 Network Settings

Configuration Profile

In the pane on the left side of the page navigate to **Onboard > Deployment and Provisioning > Configuration Profiles**.

1. Click **Create new configuration profile**
2. Enter the following details:
 - Name: byod_employee Configuration Profile
 - Networks: byod_employee Network Settings
3. Click **Save Changes**



Profile

* Name:
Enter a name for the profile.

Description:
Enter a description for the profile.

Networks:

- byod_employee Network Settings
- Example Network
- Mobile 1st Network Settings

Choose the networks to include in the profile.

Figure 95 Creating the Configuration Profile

Provisioning Settings

Navigate to **Onboard > Deployment and Provisioning > Provisioning Settings**.

1. Click **Create new provisioning settings**
2. Enter the following details:
 - Name: byod_employee Provisioning Settings
 - Organization: Aruba Networks TME
3. Click **Next**
4. The **Supported Devices** tab will be left default
5. Click **Next**

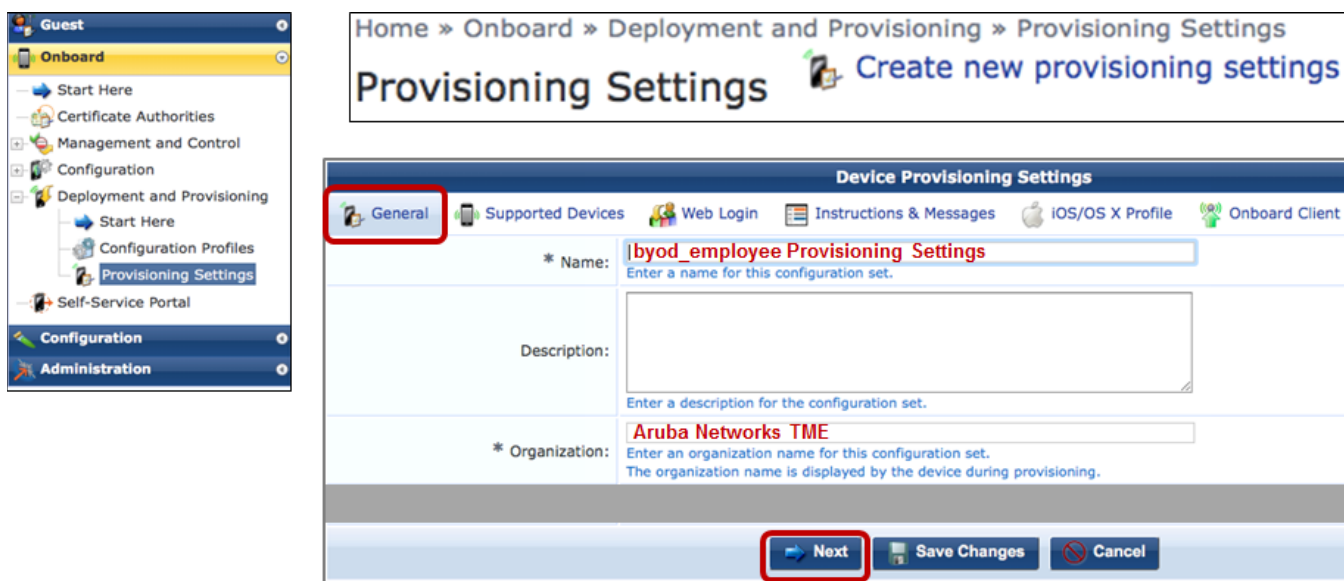


Figure 96 Creating Provisioning Settings

6. Enter the following details on the **Web Login** tab:
 - Page Name: byod_employee_onboard
 - Security Hash: Deny login on validation error – login will not be permitted
 - URL Hash Key: aruba123
 - Confirm Key: aruba123
7. Click **Next**
8. The **Instructions & Messages** tab will be left default
9. Click **Next**



Figure 97 Creating Provisioning Settings - Web Login Details

10. 1 Enter the following details on the **iOS/OS X Profile** tab

- Display Name: byod_employee Device Enrollment

11. Click **Next**

The screenshot shows the 'Device Provisioning Settings' interface. At the top, there are tabs for 'General #', 'Supported Devices', 'Web Login #', 'Instructions & Messages', 'iOS/OS X Profile' (which is selected and highlighted with a red box), 'Onboard Client', and 'Sponsorship Confirmation'. Below the tabs, the 'iOS & OS X Provisioning' section is active. It contains several fields: '* Display Name' with the value 'byod_employee Device Enrollment'; '* Profile Description' with a text area containing 'This configuration profile has network and security settings for your device to allow you to connect to the intranet and access local applications.'; '* Profile Security' with a dropdown menu set to 'Always allow removal'; and 'Edit ID' with a checkbox for 'Change the profile ID' and a note that the current profile ID is 'com.example.device.provisioning.64fff926-3e8f-40e1-9750-dad5c10df884'. Below this is the 'Profile Signing' section, which includes '* Certificate Source' set to 'Generate using the Onboard CA' and '* Common Name' set to 'Device Enrollment (Profile Signing)'. At the bottom of the form, there are four buttons: 'Previous', 'Next' (highlighted with a red box), 'Save Changes', and 'Cancel'.

Figure 98 Creating Provisioning Settings - iOS/OS X Profile Details

The Onboard Client tab is mainly used to enter configuration for older/legacy OS X devices.

12. Enter the following details on the **Onboard Client** tab:

- Provisioning Address: cp-corp (requires DNS resolution)

13. Click **Save Changes**

14. The **Sponsorship Confirmation** page can be left as default

Device Provisioning Settings

General Supported Devices Web Login Instructions & Messages iOS/OS X Profile **Onboard Client** Sponsorship Confirmation

Device Provisioning
Options for Windows, Android and Legacy OS X (10.5/6) device provisioning.
These settings are not used for iOS or OS X 10.7+ (Lion or later) devices.

* Code-Signing Certificate: None — Do not sign the application
Select a code signing certificate for signing the Windows provisioning application.

* Provisioning Address: cp-corp (requires DNS resolution)
Select the hostname or IP address to use for device provisioning.

Provisioning Access: To be provisioned, devices **must** be able to access cp-corp via HTTPS.

* Validate Certificate: Yes, validate this web server's certificate (recommended)
Specify whether the web server's certificate is to be validated during device provisioning. When testing with the default self-signed web server certificate, you may need to disable validation. This option applies to Windows, Android, and OS X 10.5/6 devices only.

Bypass Proxy: Bypass proxy server
If checked, the proxy server configured on the client will not be used during the Onboard enrollment process.

Logo Image: Select an image to use in the provisioning wizard. New images can be uploaded using the Content Manager.

* Wizard Title: Onboard Wizard
Enter a title for the wizard used on Windows and Legacy OS X (10.5/6) devices.

Password Recovery URL:
Enter the URL displayed to users who have forgotten their password.

Helpdesk URL:
Enter the URL displayed to users who require helpdesk assistance.

Previous Next **Save Changes** Cancel

Figure 99 Creating Provisioning Settings - Onboard Client Details

Navigate to **Onboard > Deployment and Provisioning > Provisioning Settings** and click **Test**.

Guest

- Onboard
 - Start Here
 - Certificate Authorities
 - Management and Control
 - Configuration
 - Deployment and Provisioning
 - Start Here
 - Configuration Profiles
 - Provisioning Settings**
 - Self-Service Portal
 - Configuration
 - Administration

Name	CA	Profile
byod_employee Provisioning Settings	byod_employee Certificate Authority	byod_employee Configuration Profile
Show Details Edit Duplicate Delete Test		
Local Device Provisioning This is the default configuration set for device provisioning.	Local Certificate Authority	Default Profile

Refresh 1 Showing 1 - 2 of 2 20 rows per page

Register Your Device

In order to connect to this network, your device must be configured for enhanced security. This wizard will guide you through the configuration process.

Login below using your Aruba TME credentials.

Register Your Device

Username:

Password:

Log In

Contact a staff member if you are experiencing difficulty logging in.

© Copyright 2018 Hewlett Packard Enterprise Development LP

Figure 100 Verifying the Provisioning Settings

PSK SSID Configuration

```
(mm01) ^[aruba] (config) #ip access-list session MobileFirst-psk-deny-client-as-dhcp-server
```

Prevent BYOD clients from acting as a DHCP server

```
(mm01) ^[aruba] (config-submode) #user any udp 68 deny
```

```
(mm01) ^[aruba] (config-submode) #ipv6 user any icmpv6 rtr-adv deny
```

```
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config) #ip access-list session MobileFirst-psk-allowall
```

Allow all other traffic to and from PSK clients

```
(mm01) ^[aruba] (config-submode) #any any any permit
```

```
(mm01) ^[aruba] (config-submode) #ipv6 any any any permit
```

```
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config) #user-role mobilefirst-authenticated
```

Create the mobilefirst-authenticated user role and apply the appropriate ACLs

```
(mm01) ^[aruba] (config-submode) #access-list session MobileFirst-psk-deny-client-as-dhcp-server
```

```
(mm01) ^[aruba] (config-submode) #access-list session MobileFirst-psk-allowall
```

```
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config-submode) #aaa authentication dot1x MobileFirst-psk
```

Define 802.1X authentication profile

```
(mm01) ^[aruba] (config-submode) #exit
```

```
(mm01) ^[aruba] (config) #aaa profile MobileFirst-psk
```

Define the AAA profile

```
(mm01) ^[aruba] (AAA Profile "MobileFirst-psk") #authentication-dot1x MobileFirst-psk
```

```
(mm01) ^[aruba] (AAA Profile "MobileFirst-psk") #initial-role MobileFirst-authenticated
```

```
(mm01) ^[aruba] (AAA Profile "MobileFirst-psk") #exit
```

```
(mm01) [aruba] (config) #wlan ssid-profile MobileFirst-psk
```

Define the SSID profile

```
(mm01) ^[aruba] (SSID Profile "MobileFirst-psk") #essid TME-MobileFirst-psk
```

```
(mm01) ^[aruba] (SSID Profile "MobileFirst-psk") #wpa-passphrase aruba123
```

```
(mm01) ^[aruba] (SSID Profile "MobileFirst-psk") #opmode wpa2-psk-aes
```

```
(mm01) ^[aruba] (SSID Profile "MobileFirst-psk") #exit
```

```
(mm01) ^[aruba] (config) #wlan virtual-ap MobileFirst-psk
```

Define the virtual AP profile and add the AAA and SSID profiles to the virtual AP profile

```
(mm01) ^[aruba] (Virtual AP profile "MobileFirst-psk") #aaa-profile MobileFirst-psk
```

```
(mm01) ^[aruba] (Virtual AP profile "MobileFirst-psk") #ssid-profile MobileFirst-psk
```

```
(mm01) ^[aruba] (Virtual AP profile "MobileFirst-psk") #vlan 96
```

```
(mm01) ^[aruba] (Virtual AP profile "MobileFirst-psk") #exit
```



```
(mm01) ^[aruba] (config) #ap-group CampusAP
(mm01) ^[aruba] (AP group "CampusAP") #virtual-ap MobileFirst-psk
(mm01) ^[aruba] (AP group "CampusAP") #exit
(mm01) ^[aruba] (config) #write memory
```

Add the virtual AP profile to the AP group

AP Configuration

```
(mm01) [aruba] (config) #whitelist-db cpsec add mac-address
a8:bd:27:c4:ae:7e
(mm01) [aruba] (config) #whitelist-db cpsec add mac-address
a8:bd:27:c4:b0:8a
(mm01) [aruba] (config) #whitelist-db cpsec add mac-address a8:bd:27:c4:ae:24
(mm01) [aruba] (config) #whitelist-db cpsec add mac-address a8:bd:27:c4:ae:0c
(mm01) [aruba] (config) #whitelist-db cpsec add mac-address a8:bd:27:c4:af:08
(mm01) [aruba] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:ae:7e ap-name
ap01 ap-group CampusAP state certified-factory-cert
(mm01) [aruba] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:b0:8a ap-name
ap02 ap-group CampusAP state certified-factory-cert
(mm01) [aruba] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:ae:24 ap-name
ap03 ap-group CampusAP state certified-factory-cert
(mm01) [aruba] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:ae:0c ap-name
ap04 ap-group CampusAP state certified-factory-cert
(mm01) [aruba] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:af:08 ap-name
ap05 ap-group CampusAP state certified-factory-cert
(mm01) [aruba] (config) #write memory
```

Whitelist the APs, assign them names, and add them to the CampusAP group

```
(mm01) [aruba] (config) #ap system-profile default
(mm01) [aruba] (AP system profile "default") #ap-console-password
aruba123
(mm01) ^[aruba] (AP system profile "default") #exit
(mm01) ^[aruba] (config) #write memory
```

Define password for AP console access

```
(mm01) [aruba] (config) #ap multizone-profile MobileFirst-
CampusAP-multizone
(mm01) ^[aruba] (AP multizone profile "MobileFirst-CampusAP-multizone") #primaryzone max-
vaps 2 max-nodes 4
(mm01) ^[aruba] (AP multizone profile "MobileFirst-CampusAP-multizone") #datazone 1
controller-ip 10.127.93.10 max-vaps 1 max-nodes 1
(mm01) ^[aruba] (AP multizone profile "MobileFirst-CampusAP-multizone") #multizone-enable
Warning: multizone can't work together with HA. Please ensure HA is disabled.
(mm01) ^[aruba] (AP multizone profile "MobileFirst-CampusAP-multizone") #exit
(mm01) ^[aruba] (config) #ap-group CampusAP
(mm01) ^[aruba] (AP group "CampusAP") #ap-multizone-profile MobileFirst-CampusAP-multizone
(mm01) ^[aruba] (AP group "CampusAP") #exit

(mm01) ^[aruba] (config) #write memory
```

Configure MultiZone

Firewall-DMZ

Initial Setup

Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...

```
'enable-debug'      : Enable auto-provisioning debug logs
'disable-debug'     : Disable auto-provisioning debug logs
'mini-setup'        : Start mini setup dialog. Provides minimal customization and
requires DHCP server
'full-setup'        : Start full setup dialog. Provides full customization
'static-activate'   : Provides customization for static or PPPOE ip assignment. Uses
activate for master information
```

Enter Option (partial string is acceptable): **full-setup**

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no):
yes

```
***** Welcome to the Aruba7010 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.
```

```
Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box
Enter System name [Aruba7010]:FW-DMZ
Enter Switch Role (standalone|md) [md]:standalone
Enter Controller VLAN ID [1]:99
Enter Controller VLAN port [GE 0/0/0]:GE 0/0/0
Enter Controller VLAN port mode (access|trunk) [access]:access
Enter VLAN interface IP address [172.16.0.254]:10.127.99.2
Enter VLAN interface subnet mask [255.255.255.0]:255.255.255.0
Enter IP Default gateway [none]:10.127.99.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
This controller is restricted, please enter country code (US|PR|GU|VI|MP|AS|FM|MH) [US]: US
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Los_Angeles
Enter Time in UTC [17:47:38]:
Enter Date (MM/DD/YYYY) [5/1/2018]:
Enter Password for admin login (up to 32 chars): aruba123
Re-type Password for admin login: aruba123
```

Current choices are:

```
System name: FW-DMZ
Switch Role: standalone
```

```
Controller VLAN id: 99
Controller VLAN port: GE 0/0/0
Controller VLAN port mode: access
VLAN interface IP address: 10.127.99.2
VLAN interface subnet mask: 255.255.255.0
IP Default gateway: 10.127.99.1
Option to configure VLAN interface IPV6 address: no
Country code: US
IANA Time Zone: America/Los_Angeles
```

```
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
Creating configuration... Done.
System will now restart!
```

Network Configuration

```
(FW-DMZ) [mynode] #configure terminal
```

```
Enter Configuration commands, one per line. End with CNTL/Z
```

```
(FW-DMZ) [mynode] (config) #vlan 93
```

```
(FW-DMZ) ^[mynode] (config-submode) #description 93-DMZ-Mgmt
```

```
(FW-DMZ) ^[mynode] (config-submode) #interface vlan 93
```

```
(FW-DMZ) ^[mynode] (config-submode) #ip address 10.127.93.1  
255.255.255.0
```

```
(FW-DMZ) ^[mynode] (config-submode) #exit
```

```
(FW-DMZ) ^[mynode] (config) #vlan 99
```

```
(FW-DMZ) ^[mynode] (config-submode) #description 99-  
Interconnect_DMZ-to-TOR
```

```
(FW-DMZ) ^[mynode] (config-submode) #interface vlan 99
```

```
(FW-DMZ) ^[mynode] (config-submode) #ip address 10.127.99.2  
255.255.255.0
```

```
(FW-DMZ) ^[mynode] (config-submode) #exit
```

```
(FW-DMZ) ^[mynode] (config) #vlan 999
```

```
(FW-DMZ) ^[mynode] (config-submode) #description 999-GuestClients
```

```
(FW-DMZ) ^[mynode] (config-submode) #interface vlan 999
```

```
(FW-DMZ) ^[mynode] (config-submode) #ip address 192.168.1.1  
255.255.255.0
```

```
(FW-DMZ) ^[mynode] (config-submode) #ip nat inside
```

```
(FW-DMZ) ^[mynode] (config-submode) #exit
```

Enter configuration mode

Add VLAN 93 for DMZ
Management with ip address

Add VLAN 99 for connectivity
to the TOR switch with ip
address

Add VLAN 999 for guest
clients with ip address

```
(FW-DMZ) ^[mynode] (config) #interface gigabitethernet 0/0/0
(FW-DMZ) ^[mynode] (config-submode) #lACP group 0 mode active
(FW-DMZ) ^[mynode] (config-submode) #lldp transmit
(FW-DMZ) ^[mynode] (config-submode) #lldp receive
(FW-DMZ) ^[mynode] (config-submode) #exit
```

Add interfaces 0/0/0 and 0/0/1 into LAG 0

```
(FW-DMZ) ^[mynode] (config) #interface gigabitethernet 0/0/1
(FW-DMZ) ^[mynode] (config-submode) #lACP group 0 mode active
(FW-DMZ) ^[mynode] (config-submode) #lldp transmit
(FW-DMZ) ^[mynode] (config-submode) #lldp receive
(FW-DMZ) ^[mynode] (config-submode) #exit
```

```
(FW-DMZ) ^[mynode] (config) #interface port-channel 0
(FW-DMZ) ^[mynode] (config-submode) #switchport mode access
(FW-DMZ) ^[mynode] (config-submode) #switchport access vlan 99
(FW-DMZ) ^[mynode] (config-submode) #exit
```

```
(FW-DMZ) ^[mynode] (config) #interface gigabitethernet 0/0/2
(FW-DMZ) ^[mynode] (config-submode) #lACP group 1 mode active
(FW-DMZ) ^[mynode] (config-submode) #lldp transmit
(FW-DMZ) ^[mynode] (config-submode) #lldp receive
(FW-DMZ) ^[mynode] (config-submode) #exit
```

Add interfaces 0/0/2 and 0/0/3 into LAG 1

```
(FW-DMZ) ^[mynode] (config) #interface gigabitethernet 0/0/3
(FW-DMZ) ^[mynode] (config-submode) #lACP group 1 mode active
(FW-DMZ) ^[mynode] (config-submode) #lldp transmit
(FW-DMZ) ^[mynode] (config-submode) #lldp receive
(FW-DMZ) ^[mynode] (config-submode) #exit
```

```
(FW-DMZ) ^[mynode] (config) #interface port-channel 1
(FW-DMZ) ^[mynode] (config-submode) #switchport mode trunk
(FW-DMZ) ^[mynode] (config-submode) #switchport trunk allowed vlan 93,999
(FW-DMZ) ^[mynode] (config-submode) #switchport trunk native vlan 93
(FW-DMZ) ^[mynode] (config-submode) #exit
```

```
(FW-DMZ) ^[mynode] (config) #snmp-server community aruba123
(FW-DMZ) ^[mynode] (config) #snmp-server host 10.127.88.20 version 2c aruba123 udp-port 162
(FW-DMZ) ^[mynode] (config) #ip default-gateway 10.127.99.1
(FW-DMZ) ^[mynode] (config) #exit
(FW-DMZ) ^[mynode] #write memory
```

Configure SNMP

SW-AGG-DMZ

```
HP-Stack-2920# configure
```

Enter configuration mode

```
HP-Stack-2920(config)# hostname SW-AGG-DMZ
```

Change the hostname

```
SW-AGG-DMZ(config)# trunk 1/1-1/2 trk1 lacp
```

```
SW-AGG-DMZ(config)# trunk 1/3-1/4 trk11 lacp
```

```
SW-AGG-DMZ(config)# trunk 1/5-1/6 trk12 lacp
```

Add ports into LAGs

```
SW-AGG-DMZ(config)# vlan 93
```

```
SW-AGG-DMZ(vlan-93)# name 93-DMZ-Mgmt
```

```
SW-AGG-DMZ(vlan-93)# untagged Trk1,Trk11-Trk12
```

```
SW-AGG-DMZ(vlan-93)# ip address 10.127.93.2 255.255.255.0
```

```
SW-AGG-DMZ(vlan-93)# exit
```

Add VLAN 93 for DMZ management untagged on trunks 1, 11, and 12 with ip address

```
SW-AGG-DMZ(config)# vlan 999
```

```
SW-AGG-DMZ(vlan-999)# name 999-GuestClients
```

```
SW-AGG-DMZ(vlan-999)# tagged Trk1,Trk11-Trk12
```

```
SW-AGG-DMZ(vlan-999)# ip address 192.168.1.2 255.255.255.0
```

```
SW-AGG-DMZ(vlan-999)# dhcp-server
```

```
SW-AGG-DMZ(vlan-999)# exit
```

Add VLAN 999 for Guest clients tagged on trunks 1, 11, and 12 with ip address and enable DHCP

```
SW-AGG-DMZ(config)# ip default-gateway 10.127.93.1
```

```
SW-AGG-DMZ(config)# snmp-server community aruba123 operator
```

```
SW-AGG-DMZ(config)# snmp-server host 10.127.88.20 community aruba123
```

```
SW-AGG-DMZ(config)# password manager user-name admin plaintext aruba123
```

```
SW-AGG-DMZ(config)# exit
```

```
SW-AGG-DMZ # write memory
```

Configure default gateway and SNMP

DMZ Configuration

MC-DMZ-01 Initial Setup

Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...

```
'enable-debug'      : Enable auto-provisioning debug logs
'disable-debug'     : Disable auto-provisioning debug logs
'mini-setup'        : Start mini setup dialog. Provides minimal customization and
requires DHCP server
'full-setup'        : Start full setup dialog. Provides full customization
'static-activate'   : Provides customization for static or PPPOE ip assignment. Uses
activate for master information
```

Enter Option (partial string is acceptable): **full-setup**

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no):
yes

```
***** Welcome to the Aruba7210 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.
```

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

```
Enter System name [Aruba7010]: mc-dmz01
Enter Switch Role (master|standalone|md) [md]: standalone
Enter Controller VLAN ID [1]: 93
Enter Controller VLAN port [GE 0/0/0]: GE 0/0/0
Enter Controller VLAN port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 93
Enter VLAN interface IP address [172.16.0.254]: 10.127.93.11
Enter VLAN interface subnet mask [255.255.255.0]: 255.255.255.0
Enter IP Default gateway [none]: 10.127.93.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
This controller is restricted, please enter country code (US|PR|GU|VI|MP|AS|FM|MH) [US]: US
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Los_Angeles
Enter Time in UTC [20:28:36]:
Enter Date (MM/DD/YYYY) [5/4/2018]:
Enter Password for admin login (up to 32 chars): aruba123
Re-type Password for admin login: aruba123
```

Current choices are:

```
System name: mc-dmz01
Switch Role: standalone
Controller VLAN id: 93
Controller VLAN port: GE 0/0/0
Controller VLAN port mode: trunk
Native VLAN id: 93
VLAN interface IP address: 10.127.93.11
VLAN interface subnet mask: 255.255.255.0
IP Default gateway: 10.127.93.1
Option to configure VLAN interface IPV6 address: no
Country code: US
IANA Time Zone: America/Los_Angeles
```

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)**yes**
Creating configuration... Done.

System will now restart!

MC-DMZ-01 Network Configuration

```
(mc-dmz01) [mynode]# configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
```

```
(mc-dmz01) [mynode] (config) #vlan 93
(mc-dmz01) ^[mynode] (config-submode) #description 93-DMZ-Mgmt
(mc-dmz01) ^[mynode] (config-submode) #exit
```

Rename VLAN 93

```
(mc-dmz01) ^[mynode] (config) #vlan 999
(mc-dmz01) ^[mynode] (config-submode) #description 999-
GuestClients
(mc-dmz01) ^[mynode] (config-submode) #exit
```

Add VLAN 999 for Guest clients

```
(mc-dmz01) ^[mynode] (config) #interface vlan 999
(mc-dmz01) ^[mynode] (config-submode) #ip address 192.168.1.11
255.255.255.0
(mc-dmz01) ^[mynode] (config-submode) #exit
```

Add ip address for VLAN 999 (required for captive portal redirection)

```
(mc-dmz01) ^[mynode] (config) #interface gigabitethernet 0/0/0
(mc-dmz01) ^[mynode] (config-submode) #lacp group 0 mode active
(mc-dmz01) ^[mynode] (config-submode) #lldp transmit
(mc-dmz01) ^[mynode] (config-subconfig-submode) #exit
```

Add interface 0/0/0 and 0/0/1 into LAG 0

```
(mc-dmz01) ^[mynode] (config)# interface gigabitethernet 0/0/1
(mc-dmz01) ^[mynode] (config-submode)# lACP group 0 mode active
(mc-dmz01) ^[mynode] (config-submode)# lldp transmit
(mc-dmz01) ^[mynode] (config-submode)# lldp receive
(mc-dmz01) ^[mynode] (config-submode)# exit

(mc-dmz01) ^[mynode] (config) #interface port-channel 0
(mc-dmz01) ^[mynode] (config-submode) #switchport mode trunk
(mc-dmz01) ^[mynode] (config-submode) #switchport trunk allowed vlan 93,999
(mc-dmz01) ^[mynode] (config-submode) #switchport trunk native vlan 93
(mc-dmz01) ^[mynode] (config-submode) #exit

(mc-dmz01) ^[mynode] (config) #vrrp 93
(mc-dmz01) ^[mynode] (config-submode) #ip address 10.127.93.10
(mc-dmz01) ^[mynode] (config-submode) #priority 110
(mc-dmz01) ^[mynode] (config-submode) #vlan 93
(mc-dmz01) ^[mynode] (config-submode) #no shutdown
(mc-dmz01) ^[mynode] (config-submode) #exit

(mc-dmz01) ^[mynode] (config) #master-redundancy
(mc-dmz01) ^[mynode] (config-submode) #master-vrrp 93
(mc-dmz01) ^[mynode] (config-submode) #peer-ip-address
10.127.93.12 ipsec aruba123
(mc-dmz01) ^[mynode] (config-submode) #exit
(mc-dmz01) ^[mynode] (config) #write memory
```

Configure VRRP

MC-DMZ-02 Initial Setup

Auto-provisioning is in progress. It requires DHCP and Activate servers

Choose one of the following options to override or debug auto-provisioning...

```
'enable-debug'      : Enable auto-provisioning debug logs
'disable-debug'     : Disable auto-provisioning debug logs
'mini-setup'        : Start mini setup dialog. Provides minimal customization and
requires DHCP server
'full-setup'        : Start full setup dialog. Provides full customization
'static-activate'   : Provides customization for static or PPPOE ip assignment. Uses
activate for master information
```

9

Enter Option (partial string is acceptable): **full-setup**

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no):
yes

```
***** Welcome to the Aruba7210 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.
```

```
Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box
```

```
Enter System name [Aruba7210]: mc-dmz02
Enter Switch Role (master|standalone|md) [md]: standalone
Enter Controller VLAN ID [1]: 93
Enter Controller VLAN port [GE 0/0/0]: GE 0/0/0
Enter Controller VLAN port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 93
Enter VLAN interface IP address [172.16.0.254]: 10.127.93.12
Enter VLAN interface subnet mask [255.255.255.0]: 255.255.255.0
Enter IP Default gateway [none]: 10.127.93.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
This controller is restricted, please enter country code (US|PR|GU|VI|MP|AS|FM|MH) [US]: US
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Los_Angeles
Enter Time in UTC [20:28:36]:
Enter Date (MM/DD/YYYY) [5/4/2018]:
Enter Password for admin login (up to 32 chars): aruba123
Re-type Password for admin login: aruba123
```

Current choices are:

System name: mc-dmz02

```
Switch Role: standalone
Controller VLAN id: 93
Controller VLAN port: GE 0/0/0
Controller VLAN port mode: trunk
Native VLAN id: 93
VLAN interface IP address: 10.127.93.12
VLAN interface subnet mask: 255.255.255.0
IP Default gateway: 10.127.93.1
Option to configure VLAN interface IPV6 address: no
Country code: US
IANA Time Zone: America/Los_Angeles
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
Creating configuration... Done.
System will now restart!
```

MC-DMZ-02 Network Configuration

```
(mc-dmz02) [mynode] #configure terminal
```

Enter configuration mode

Enter Configuration commands, one per line. End with CNTL/Z

```
(mc-dmz02) [mynode] (config) #vlan 93
```

Rename VLAN 93

```
(mc-dmz02) ^[mynode] (config-submode) #description 93-DMZ-Mgmt
```

```
(mc-dmz02) ^[mynode] (config-submode) #exit
```

```
(mc-dmz02) ^[mynode] (config) #vlan 999
```

Add VLAN 999 for Guest clients

```
(mc-dmz02) ^[mynode] (config-submode) #description 999-GuestClients
```

```
(mc-dmz02) ^[mynode] (config-submode) #exit
```

```
(mc-dmz02) ^[mynode] (config) #interface vlan 999
```

Add ip address for VLAN 999 (required for captive portal redirection)

```
(mc-dmz02) ^[mynode] (config-submode) #ip address 192.168.1.12 255.255.255.0
```

```
(mc-dmz02) ^[mynode] (config-submode) #exit
```

```
(mc-dmz02) ^[mynode] (config) #interface gigabitethernet 0/0/0
```

Add interface 0/0/0 and 0/0/1 into LAG 0

```
(mc-dmz02) ^[mynode] (config-submode) #lACP group 0 mode active
```

```
(mc-dmz02) ^[mynode] (config-submode) #lldp transmit
```

```
(mc-dmz02) ^[mynode] (config-submode) #exit
```

```
(mc-dmz02) ^[mynode] (config) #interface gigabitethernet 0/0/1
```

```
(mc-dmz02) ^[mynode] (config-submode) #lACP group 0 mode active
```

```
(mc-dmz02) ^[mynode] (config-submode) #lldp transmit
```

```
(mc-dmz02) ^[mynode] (config-submode) #lldp receive
```

```
(mc-dmz02) ^[mynode] (config-submode) #exit
```

```
(mc-dmz02) ^[mynode] (config) #interface port-channel 0
```

```
(mc-dmz02) ^[mynode] (config-submode) #switchport mode trunk
```

```
(mc-dmz02) ^[mynode] (config-submode) #switchport trunk allowed vlan 93,999
```

```
(mc-dmz02) ^[mynode] (config-submode) #switchport trunk native vlan 93
```

```
(mc-dmz02) ^[mynode] (config-submode) #exit
```

```
(mc-dmz02) ^[mynode] (config) #vrrp 93
```

Configure VRRP

```
(mc-dmz02) ^[mynode] (config-submode) #ip address 10.127.93.10
```

```
(mc-dmz02) ^[mynode] (config-submode) #priority 100
```

```
(mc-dmz02) ^[mynode] (config-submode) #vlan 93
```

```
(mc-dmz02) ^[mynode] (config-submode) #no shutdown
```

```
(mc-dmz02) ^[mynode] (config-submode) #exit
```

```
(mc-dmz02) ^[mynode] (config) #master-redundancy
(mc-dmz02) ^[mynode] (config-submode) #master-vrrp 93
(mc-dmz02) ^[mynode] (config-submode) #peer-ip-address 10.127.93.11 ipsec aruba123
(mc-dmz02) ^[mynode] (config-submode) #exit
```

```
(mc-dmz02) ^[mynode] (config) #write memory
```

MC-DMZ-01 Licenses

```
(mc-dmz01) [mynode] #configure terminal
```

Enter configuration mode

```
(mc-dmz01) [mynode] (config) #cd /mm
```

Navigate to /mm system level

```
(mc-dmz01) ^[mm] (config) #license add s5nBnaCi-ZUGO1WHb-L7suags6-gjivLuQA-X9yrCy2a-tVY
```

Add Lic-PEF license

Please make sure to enable the feature bit to have the license take effect.

```
(mc-dmz01) ^[mm] (config) #show license-pool-profile-root
```

Show command indicates feature bit must be enabled

```
License root(/) pool profile
```

```
-----
Parameter          Value
-----
enable PEFNG feature Disabled
enable RFP feature  Disabled
enable ACR feature  Disabled
enable WebCC feature Disabled
```

```
(mc-dmz01) ^[mm] (config) #license-pool-profile-root
```

```
(mc-dmz01) ^[mm] (License root(/) pool profile) #pefng-licenses-enable
```

Enable the feature bit for Lic-PEF

```
(mc-dmz01) ^[mm] (License root(/) pool profile) #exit
```

```
(mc-dmz01) [mm] (config) #write memory
```

```
(mc-dmz01) [mm] (config) #show license-pool-profile-root
```

Verify that license has been enabled

```
License root(/) pool profile
```

```
-----
Parameter          Value
-----
enable PEFNG feature Enabled
enable RFP feature  Disabled
enable ACR feature  Disabled
enable WebCC feature Disabled
```

MC-DMZ-01 Guest WLAN

```
(mc-dmz01) [mynode] (config) #cd /mm
```

Navigate to the /mm system level

```
(mc-dmz01) [mm] (config) #database synchronize period 60
```

Set the database synchronization interval

```
(mc-dmz01) ^[mm] (config) #ntp server 10.127.32.10
```

Set the NTP server

```
(mc-dmz01) ^[mm] (config) #snmp-server community aruba123
```

Configure SNMP

```
(mc-dmz01) ^[mm] (config) #snmp-server host 10.127.88.20 version 2c aruba123
```

```
(mc-dmz01) ^[mm] (config) #mgmt-server primary-server  
10.127.88.20 profile default-amp
```

Designate AirWave for management

```
(mc-dmz01) ^[mm] (config) #firewall-visibility
```

```
(mc-dmz01) ^[mm] (config) #firewall dpi
```

Add firewall visibility

Warning: Application visibility/control is enabled, this change would take effect after reloading the controller(s) in "/mm"

```
(mc-dmz01) ^[mm] (config) #netdestination guest-dmz-external-  
captive-portal
```

Create alias for the captive portal

```
(mc-dmz01) ^[mm] (config-submode) #host 10.127.93.30
```

```
(mc-dmz01) ^[mm] (config-submode) #exit
```

```
(mc-dmz01) ^[mm] (config) #netdestination guest-dmz-internal-net
```

Create alias for the internal DMZ network

```
(mc-dmz01) ^[mm] (config-submode) #network 10.0.0.0 255.0.0.0
```

```
(mc-dmz01) ^[mm] (config-submode) #network 192.168.0.0 255.255.0.0
```

```
(mc-dmz01) ^[mm] (config-submode) #exit
```

```
(mc-dmz01) ^[mm] (config) #ip access-list session guest-dmz-  
allow-external-captive-portal
```

Permit http and https traffic to captive portal

```
(mc-dmz01) ^[mm] (config-submode) #user alias guest-dmz-external-  
captive-portal svc-http permit
```

```
(mc-dmz01) ^[mm] (config-submode) #user alias guest-dmz-external-captive-portal svc-https  
permit
```

```
(mc-dmz01) ^[mm] (config-submode) #exit
```

```
(mc-dmz01) ^[mm] (config) #ip access-list session guest-dmz-block
```

Block client traffic to the internal network

```
(mc-dmz01) ^[mm] (config-submode) #user alias guest-dmz-internal-net any deny
```

```
(mc-dmz01) ^[mm] (config-submode) #exit
```

```
(mc-dmz01) ^[mm] (config) #ip access-list session guest-dmz-  
cplogout  
(mc-dmz01) ^[mm] (config-submode) #user alias controller svc-  
https dst-nat 8081  
(mc-dmz01) ^[mm] (config-submode) #exit
```

Permit redirect to controller
after successful guest
registration

```
(mc-dmz01) ^[mm] (config) #ip access-list session guest-dmz-  
authenticated  
(mc-dmz01) ^[mm] (config-submode) #any any svc-http permit  
(mc-dmz01) ^[mm] (config-submode) #any any svc-https permit  
(mc-dmz01) ^[mm] (config-submode) #exit
```

Permit http and https traffic

```
(mc-dmz01) ^[mm] (config) #ip access-list session guest-dmz-drop-  
all  
(mc-dmz01) ^[mm] (config-submode) #user any any deny log position 1  
(mc-dmz01) ^[mm] (config-submode) #exit
```

Deny all traffic not explicitly
permitted by other ACLs

```
(mc-dmz01) ^[mm] (config) #user-role guest-dmz  
(mc-dmz01) ^[mm] (config-submode) #access-list session guest-dmz-cplogout position 3  
(mc-dmz01) ^[mm] (config-submode) #access-list session logon-control position 4  
(mc-dmz01) ^[mm] (config-submode) #access-list session guest-dmz-block position 5  
(mc-dmz01) ^[mm] (config-submode) #access-list session guest-dmz-authenticated position 6  
(mc-dmz01) ^[mm] (config-submode) #access-list session guest-dmz-drop-all position 7  
(mc-dmz01) ^[mm] (config-submode) #exit
```

Create guest-dmz user role and apply ACLs

```
(mc-dmz01) ^[mm] (config) #user-role guest-dmz-logon  
(mc-dmz01) ^[mm] (config-submode) #access-list session guest-dmz-  
allow-external-captive-portal position 3  
(mc-dmz01) ^[mm] (config-submode) #access-list session logon-control position 4  
(mc-dmz01) ^[mm] (config-submode) #access-list session captiveportal position 5  
(mc-dmz01) ^[mm] (config-submode) #exit
```

Create guest-dmz-logon user
role and apply ACLs

```
(mc-dmz01) ^[mm] (config) #aaa authentication-server radius CP-DMZ  
(mc-dmz01) ^[mm] (RADIUS Server "CP-DMZ") #host 10.127.93.30  
(mc-dmz01) ^[mm] (RADIUS Server "CP-DMZ") #key aruba123  
(mc-dmz01) ^[mm] (RADIUS Server "CP-DMZ") #mac-delimiter colon  
(mc-dmz01) ^[mm] (RADIUS Server "CP-DMZ") #exit
```

Designate RADIUS server

```
(mc-dmz01) ^[mm] (config) #aaa rfc-3576-server 10.127.93.30  
(mc-dmz01) ^[mm] (RFC 3576 Server "10.127.93.30") #key aruba123  
(mc-dmz01) ^[mm] (RFC 3576 Server "10.127.93.30") #exit
```

Designate RFC 3576 server

```
(mc-dmz01) ^[mm] (config) #aaa server-group CP-DMZ  
(mc-dmz01) ^[mm] (Server Group "CP-DMZ") #auth-server CP-DMZ
```

Define AAA server group

```
(mc-dmz01) ^[mm] (Server Group "CP-DMZ") #exit
```

```
(mc-dmz01) ^[mm] (config) #aaa authentication mac guest-dmz
```

```
(mc-dmz01) ^[mm] (MAC Authentication Profile "guest-dmz")  
#delimiter colon
```

Define MAC authentication profile

```
(mc-dmz01) ^[mm] (MAC Authentication Profile "guest-dmz") #case upper
```

```
(mc-dmz01) ^[mm] (MAC Authentication Profile "guest-dmz") #exit
```

```
(mc-dmz01) ^[mm] (config) #aaa authentication captive-portal  
guest-dmz
```

Define captive portal profile

```
(mc-dmz01) ^[mm] (Captive Portal Authentication Profile "guest-dmz") #login-page  
https://cp-dmz.aruba-tme.com/guest/guest_registration.php
```

```
(mc-dmz01) ^[mm] (Captive Portal Authentication Profile "guest-dmz") #welcome-page  
/auth/welcome.html
```

```
(mc-dmz01) ^[mm] (Captive Portal Authentication Profile "guest-dmz") #no guest-logon
```

```
(mc-dmz01) ^[mm] (Captive Portal Authentication Profile "guest-dmz") #redirect-pause 3
```

```
(mc-dmz01) ^[mm] (Captive Portal Authentication Profile "guest-dmz") #server-group CP-DMZ
```

```
(mc-dmz01) ^[mm] (Captive Portal Authentication Profile "guest-dmz") #default-role guest-  
dmz-logon
```

```
(mc-dmz01) ^[mm] (Captive Portal Authentication Profile "guest-dmz") #exit
```

```
(mc-dmz01) ^[mm] (config) #user-role guest-dmz-logon
```

```
(mc-dmz01) ^[mm] (config-submode) #captive-portal guest-dmz
```

```
(mc-dmz01) ^[mm] (config-submode) #exit
```

Apply captive portal profile to the guest-dmz-logon role

```
(mc-dmz01) ^[mm] (config) #aaa profile guest-dmz
```

Define the AAA profile

```
(mc-dmz01) ^[mm] (AAA Profile "guest-dmz") #initial-role guest-dmz-logon
```

```
(mc-dmz01) ^[mm] (AAA Profile "guest-dmz") #mac-default-role guest-dmz
```

```
(mc-dmz01) ^[mm] (AAA Profile "guest-dmz") #radius-accounting CP-DMZ
```

```
(mc-dmz01) ^[mm] (AAA Profile "guest-dmz") #rfc-3576-server 10.127.93.30
```

```
(mc-dmz01) ^[mm] (AAA Profile "guest-dmz") #authentication-mac guest-dmz
```

```
(mc-dmz01) ^[mm] (AAA Profile "guest-dmz") #mac-server-group CP-DMZ
```

```
(mc-dmz01) ^[mm] (AAA Profile "guest-dmz") #exit
```

```
(mc-dmz01) ^[mm] (config) #wlan ssid-profile MobileFirst-guest
```

Define the SSID profile

```
(mc-dmz01) ^[mm] (SSID Profile "MobileFirst-guest") #essid TME-MobileFirst-guest
```

```
(mc-dmz01) ^[mm] (SSID Profile "MobileFirst-guest") #opmode opensystem
```

```
(mc-dmz01) ^[mm] (SSID Profile "MobileFirst-guest") #exit
```

```
(mc-dmz01) ^[mm] (config) #wlan virtual-ap MobileFirst-guest
```

Define the virtual AP profile

```
(mc-dmz01) ^[mm] (Virtual AP profile "MobileFirst-guest") #aaa-profile guest-dmz
```

```
(mc-dmz01) ^[mm] (Virtual AP profile "MobileFirst-guest") #ssid-profile MobileFirst-guest
```

```
(mc-dmz01) ^[mm] (Virtual AP profile "MobileFirst-guest") #vlan 999
```

```
(mc-dmz01) ^[mm] (Virtual AP profile "MobileFirst-guest") #forward-mode tunnel
```

```
(mc-dmz01) ^[mm] (Virtual AP profile "MobileFirst-guest") #exit
```

```
(mc-dmz01) ^[mm] (config) # ap-group CampusAP
(mc-dmz01) ^[mm] (AP group "CampusAP") #virtual-ap MobileFirst-guest
(mc-dmz01) ^[mm] (AP group "CampusAP") #exit
```

Define the AP group

```
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec add mac-address
a8:bd:27:c4:ae:7e
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec add mac-address
a8:bd:27:c4:b0:8a
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec add mac-address a8:bd:27:c4:ae:24
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec add mac-address a8:bd:27:c4:ae:0c
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec add mac-address a8:bd:27:c4:af:08
```

Whitelist the APs, assign them names, and add them to the CampusAP group

```
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:ae:7e ap-name
ap01 ap-group CampusAP state certified-factory-cert cert-type factory-cert
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:b0:8a ap-name
ap02 ap-group CampusAP state certified-factory-cert cert-type factory-cert
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:ae:24 ap-name
ap03 ap-group CampusAP state certified-factory-cert cert-type factory-cert
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:ae:0c ap-name
ap04 ap-group CampusAP state certified-factory-cert cert-type factory-cert
(mc-dmz01) ^[mm] (config) #whitelist-db cpsec modify mac-address a8:bd:27:c4:af:08 ap-name
ap05 ap-group CampusAP state certified-factory-cert cert-type factory-cert
(mc-dmz01) ^[mm] (config) #write memory
```

Saving Configuration...

Configuration Saved.

HTTPS Server Certificate for DMZ MCs

Uploading a public HTTPS server certificate is more secure and provides an enhanced client onboarding experience for users connecting to SSIDs that utilize captive portal redirection. Clients should be redirected to webpages with certificates that are natively trusted. In the Aruba test network used for the Mobile First Base Designs Lab for ArubaOS 8, a public wildcard certificate *.aruba-tme.com is used on all Mobility Controllers. Using the public wildcard certificate improves the client onboarding experience in the employee and guest SSIDs since both utilize a captive portal.

Certificates can be uploaded using the following steps:

1. Log into the MM01 GUI
2. Select the hierarchy path **/Managed Network/aruba**
3. Navigate to **Configuration > System > Certificates**
4. Under Import Certificates, click the **+** button to bring up the New Certificate window
5. Browse to your certificate and fill in the fields
6. Click Submit to save.

General Admin AirWave CPSec **Certificates** SNMP Logging Profiles More

▼ Import Certificates

NAME	TYPE	FILENAME	REFERENCES	EXPIRED
master-ssh-pub-cert	PublicCert	master-ssh-pub-cert	--	--
STAR_aruba-tme_com	ServerCert	star_aruba-tme_com.pfx	--	--

+

New Certificate

Certificate name: STAR_aruba-tme_com

Certificate filename: star_aruba-tme_com.pfx

Optional passphrase:

Retype passphrase:

Certificate format: DER

Certificate type: CRL

> Export Certificates
> CSR

Figure 101 Uploading HTTPS Server Certificate via GUI

The certificate will be uploaded at this point to the four mobility controllers in the hierarchy. Use the following steps to assign the newly uploaded certificate to be used by the controller:

1. Select the hierarchy path **/Managed Network/aruba**
2. Navigate to **Configuration > System > Profiles > Other Profiles > Web Server Configuration**
 - Use the drop-down to select the newly uploaded certificate for Captive Portal
 - Optionally, use the same certificate for the switch
3. Click Submit to save and apply these changes to the four mobility controllers.

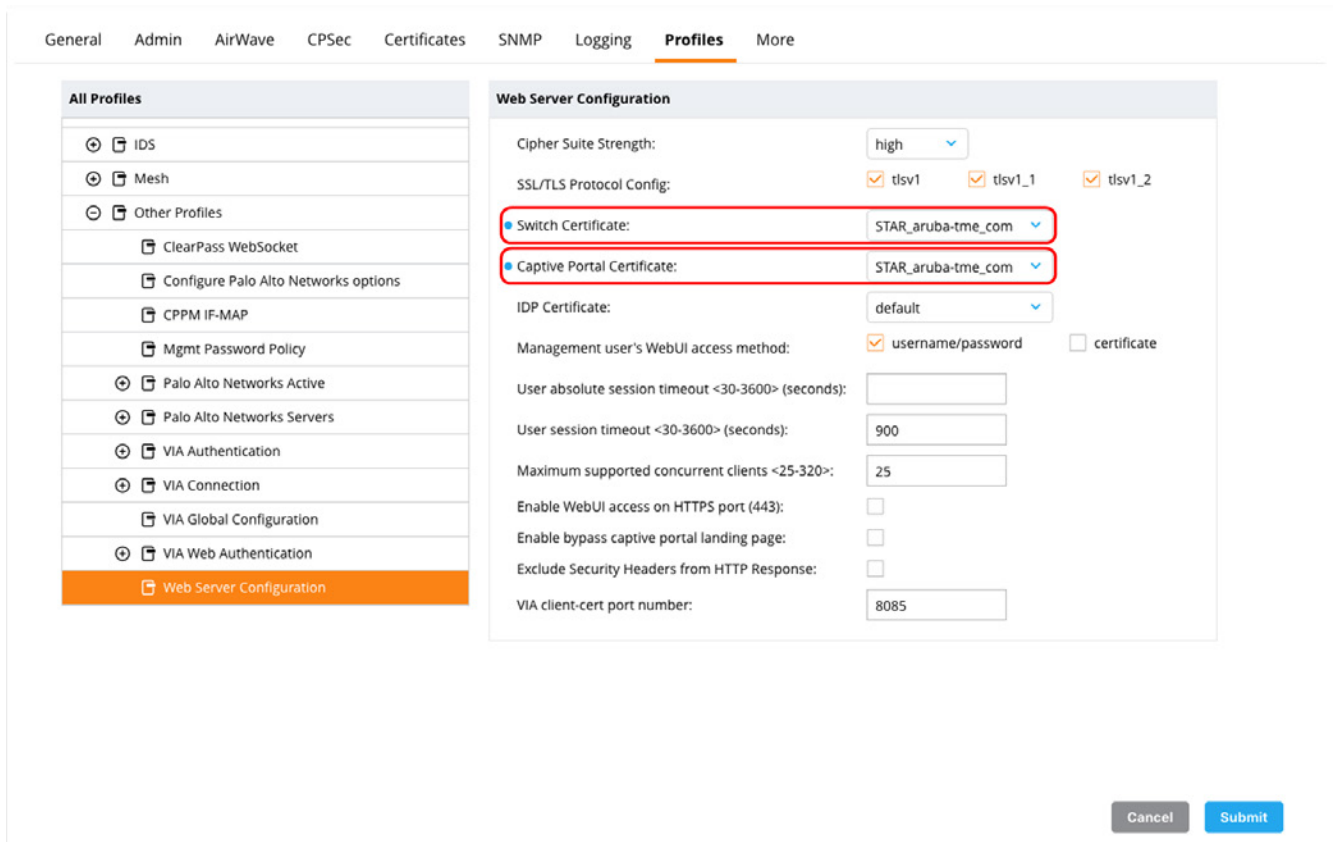


Figure 102 Assigning the Certificate to the Controller

Guest ClearPass Configuration

CP-DMZ

Navigate to the address of CP-DMZ in a web browser. Open ClearPass and log in. The default credentials for ClearPass are admin/eTIPS123.

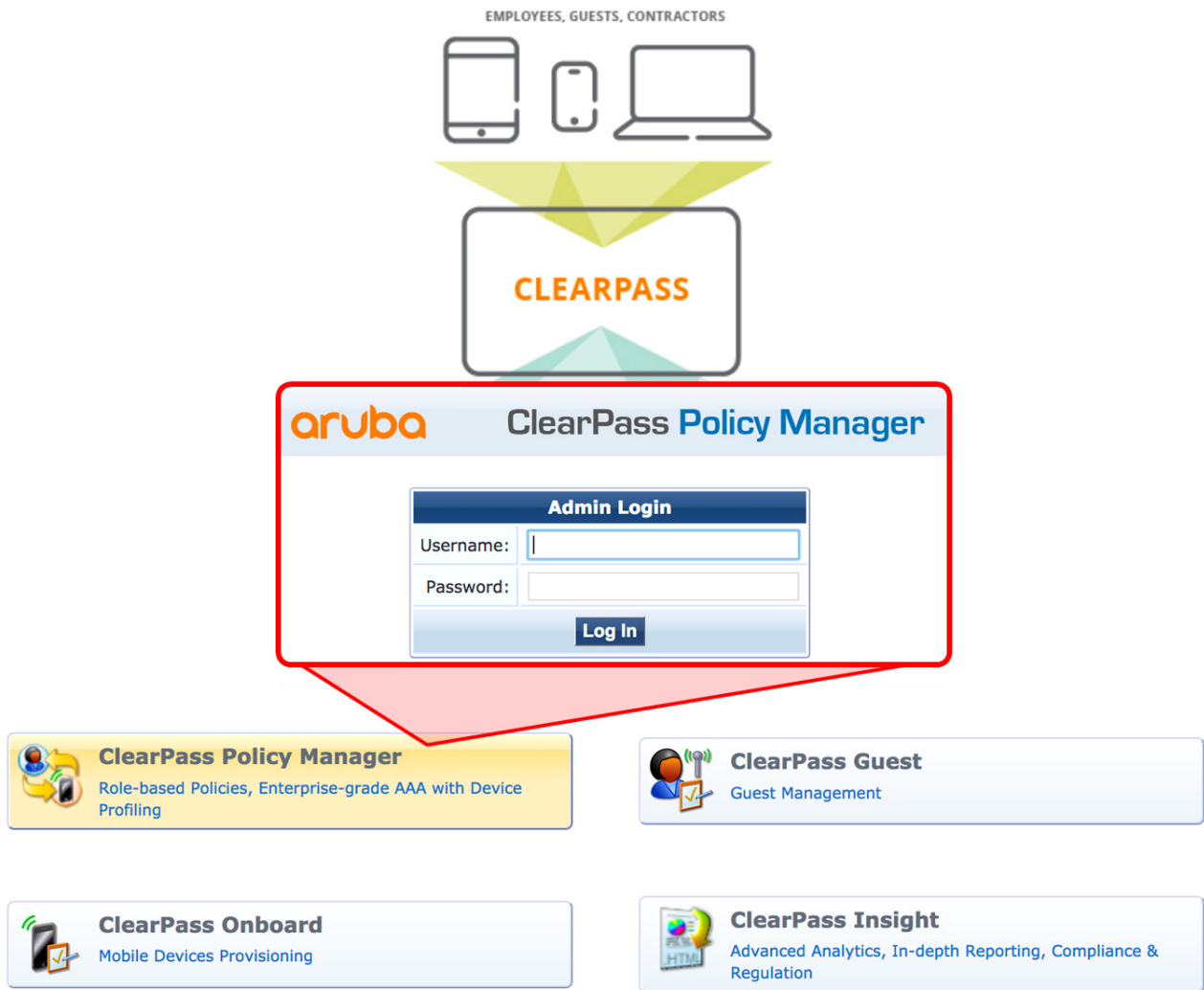


Figure 103 Log in to ClearPass

In the Mobile First Base Designs Lab for ArubaOS 8 test network CP-Corp is configured as seen in **Administration > Server Manager > Server Configuration > cp-dmz**.

		IPv4	IPv6	Action
Management Port	IP Address	10.127.93.30		Configure
	Subnet Mask	255.255.255.0		
	Default Gateway	10.127.93.1		
Data/External Port	IP Address			Configure
	Subnet Mask			
	Default Gateway			
DNS Settings	Primary	10.127.3.11		Configure
	Secondary	10.127.3.12		
	Tertiary			

Figure 104 ClearPass Server Configuration

Trust List and Certificates

In order to upload the publicly signed HTTPS Server Certificate, the Trust List for the certificate must be uploaded first.

1. Navigate to **Administration > Certificates > Trust List**
2. Click **Add**
3. In the pop-up window select the root CA certificate file and click **Add Certificate**
4. Repeat the steps above for any intermediate CA certificates applicable to your HTTPS Server Certificate

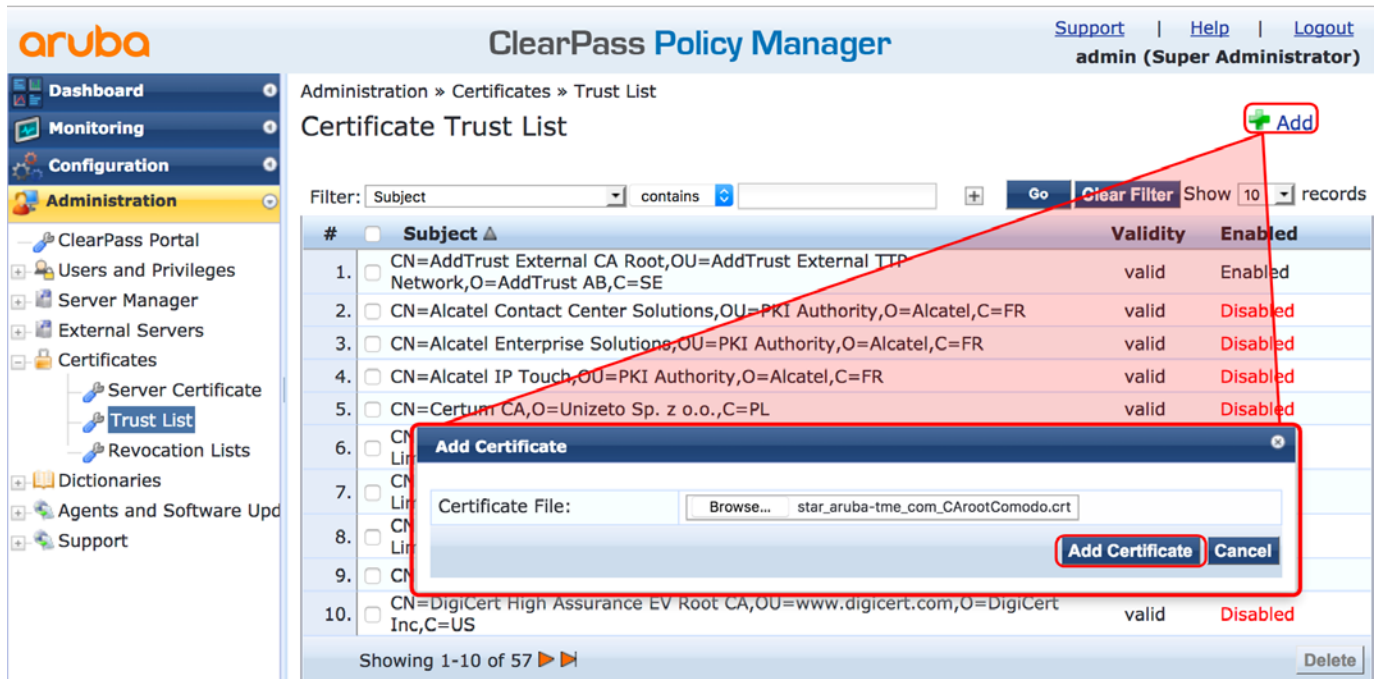


Figure 105 Add and Enable the Trust List

Next the Server Certificate must be uploaded. Errors will prevent the certificate from being imported if the Trust List requirement is not met first.

1. Navigate to **Administration > Certificates > Server Certificate**
2. Choose **HTTPS Server Certificate** under the **Select Type** dropdown
3. Click **Import Server Certificate**
4. Browse for the Certificate File
5. Brose for the Private Key File
6. Enter the Private Key Password
7. Click **Import**

The screenshot displays the Aruba ClearPass Policy Manager interface. The left sidebar shows the navigation menu with 'Administration' selected. The main content area is titled 'Server Certificate' and shows details for a certificate issued to 'O=PolicyManager, CN=cp-dmz'. The 'Import Server Certificate' option is highlighted in the top right menu. A modal window titled 'Import Server Certificate' is open, showing fields for 'Selected Server' (cp-dmz), 'Selected Type' (HTTPS Server Certificate), 'Certificate File' (star_aruba-tme_com.crt), 'Private Key File' (star_aruba-tme_com.key), and 'Private Key Password'. The 'Import' button is highlighted.

Server Certificate updated successfully. Please log in again to continue...

Figure 106 *Uploading the Server Certificate*

Upon successful import, there will be a confirmation message. You will have to log out of ClearPass Policy Manager and log in again.

Network Devices

Navigate to **Configuration > Network > Devices**. Click **Add** in the top-right corner to add controllers to the list. Note that the MCs have been added in a cluster using an IP range of 10.127.93.11-12.

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'ClearPass Policy Manager' and shows the path 'Configuration > Network > Devices'. A table lists network devices, with one entry: 'DMZ Mobility Controllers' with IP range '10.127.93.11-12'. An 'Add' button is highlighted with a red box in the top right corner. The 'Add Device' dialog box is open, showing the following fields:

Device	SNMP Read Settings	SNMP Write Settings	CLI Settings
Name:	DMZ Mobility Controllers		
IP or Subnet Address:	10.127.93.11-12 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)		
Description:	Mobility controllers in DMZ to serve guest WiFi.		
RADIUS Shared Secret:	aruba123	Verify:	aruba123
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Aruba		
Enable RADIUS CoA:	<input checked="" type="checkbox"/>	RADIUS CoA Port:	3799
Attributes			
Attribute	Value		
1. Click to add...			

The 'Add' button is highlighted with a red box in the bottom right corner of the dialog.

Figure 107 Adding DMZ Controllers as Devices to ClearPass

Guest Authentication with MAC Caching Wizard

Navigate to **Configuration > Start Here**. Click **Guest Authentication with MAC Caching** to begin the wizard. Self-Registration will be added later when the Captive Portal is configured. Go through the wizard using the tabs, filling in the fields as follows. Everything else can be left blank or use the default value.

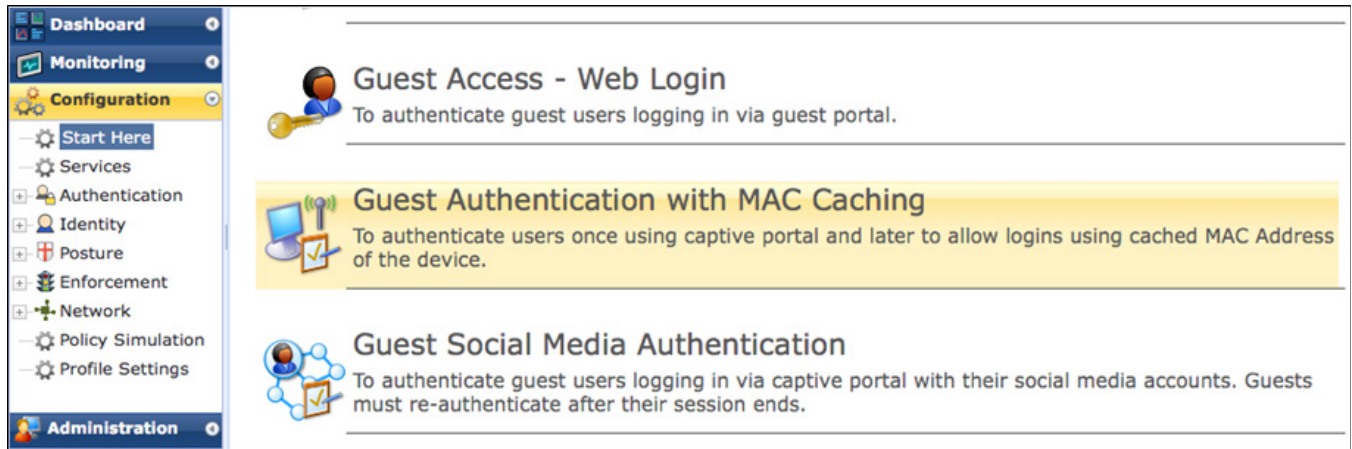


Figure 108 Guest Authentication with MAC Caching

General

1. Navigate to the **General** tab
2. Enter guest-dmz as the **Name Prefix**
3. Click **Next**

The screenshot shows the 'General' tab of the 'MAC Caching Settings' wizard. At the top are five tabs: General, Wireless Network Settings, MAC Caching Settings, Posture Settings, and Access Restrictions. The 'General' tab is active. It contains a 'Select Prefix:' dropdown menu set to 'Select' and a 'Name Prefix*:' text input field containing 'guest-dmz'. Below these is a 'Description' section with a text area containing the following text: 'Users first login via captive portal and their MAC addresses are cached. Subsequent logins will use MAC authentication and bypass the captive portal. Network access can be restricted based on day of the week, bandwidth limit or number of unique devices used by the User. The cache lifetime of the MAC address can vary according to the user's role (Guest, Employee or Contractor) and after that the user will have to re-authenticate via captive portal. Posture checks can be enabled, optionally, to validate the client device for AntiVirus, AntiSpyware, Firewall status. These results will determine the enforcement for the device.' At the bottom of the form are five buttons: 'Back to Start Here' (with a left arrow), 'Delete', 'Next >' (highlighted with a red box), 'Add Service', and 'Cancel'.

Figure 109 General Tab

Wireless Network Settings

1. Navigate to the **Wireless Network Settings** tab
2. Enter the following details:
 - Wireless SSID: TME-MobileFirst-Guest
 - Select Wireless Controller: DMZMaster-VIP
3. Everything else can be left as default
4. Click **Next**

General | **Wireless Network Settings** | MAC Caching Settings | Posture Settings | Access Restrictions

Select a wireless controller from the list, or create a new one

Wireless SSID*:	TME-MobileFirst-guest
Select Wireless Controller:	DMZ Mobility Controllers
Wireless Controller Name:	DMZ Mobility Controllers
Controller IP Address:	10.127.93.10-12
Vendor Name:	Aruba
RADIUS Shared Secret:
Enable RADIUS CoA:	<input checked="" type="checkbox"/> Automatically filled from Device List
RADIUS CoA Port:	3799

[Back to Start Here](#) | Delete | **Next >** | Update Service | Cancel

Figure 110 Wireless Network Settings Tab

MAC Caching Settings

1. Navigate to the **MAC Caching Settings** tab
2. Enter *One Day* for **Cache duration for Guest**
3. Click **Next**

General | **Wireless Network Settings** | **MAC Caching Settings** | Posture Settings | Access Restrictions

Enter MAC Caching duration for the users. After this time expires, users will have to re-authenticate via captive portal

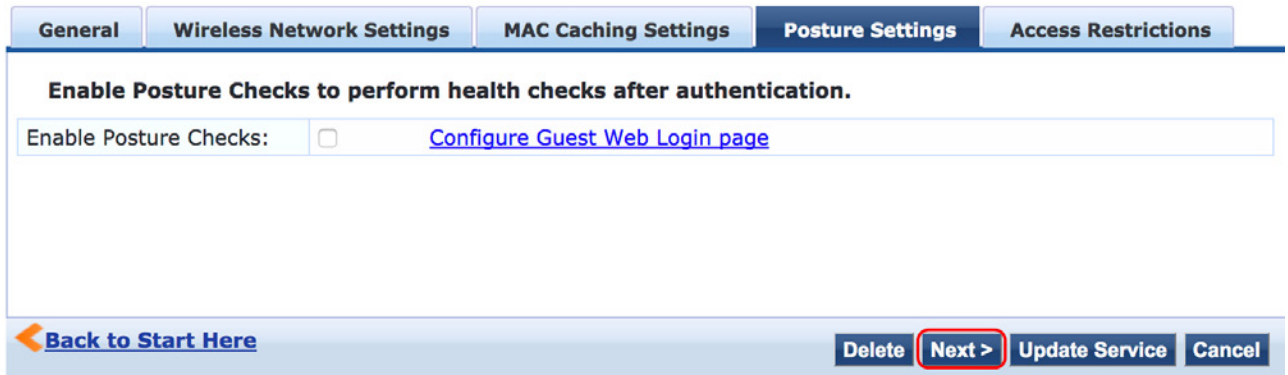
Cache duration for Employee:	Account Expiry Time
Cache duration for Guest:	One Day
Cache duration for Contractor:	Account Expiry Time

[Back to Start Here](#) | Delete | **Next >** | Update Service | Cancel

Figure 111 MAC Caching Settings Tab

Posture Settings

1. Leave the **Posture Settings** tab blank
2. Click **Next**

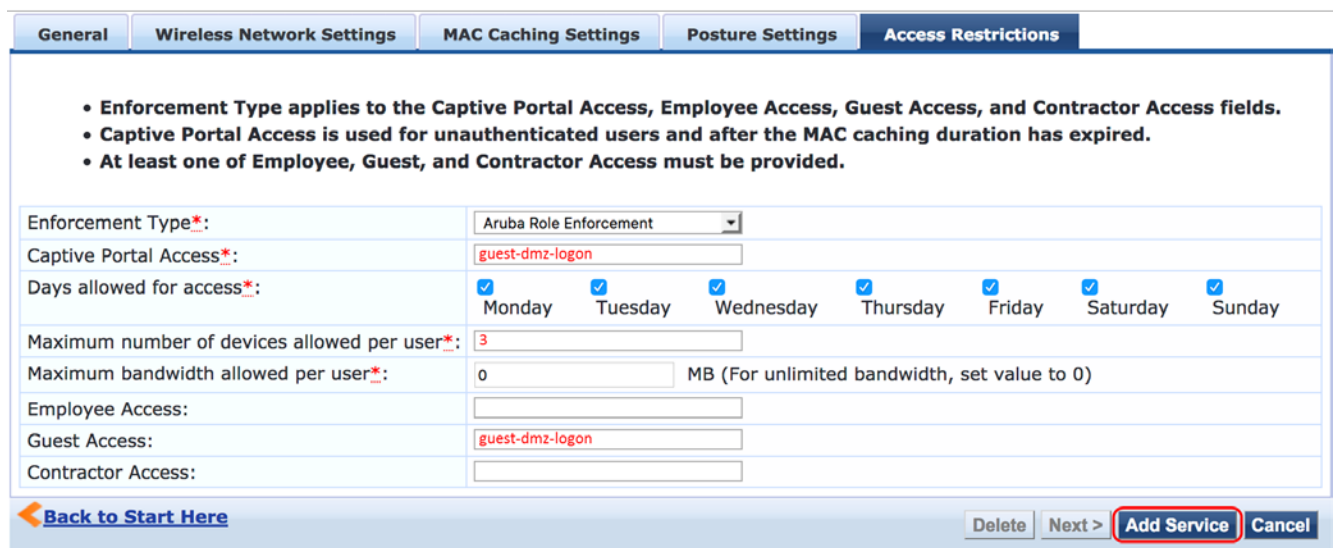


The screenshot shows the 'Posture Settings' tab selected in a configuration interface. The interface has a top navigation bar with tabs: 'General', 'Wireless Network Settings', 'MAC Caching Settings', 'Posture Settings', and 'Access Restrictions'. Below the tabs, there is a heading: 'Enable Posture Checks to perform health checks after authentication.' A form field labeled 'Enable Posture Checks:' contains an unchecked checkbox and a link 'Configure Guest Web Login page'. At the bottom of the interface, there are buttons: 'Back to Start Here', 'Delete', 'Next >', 'Update Service', and 'Cancel'. The 'Next >' button is highlighted with a red box.

Figure 112 Posture Settings Tab

Access Restrictions

1. Navigate to the **Access Restrictions** tab
2. Enter the following values:
 - Enforcement Type: Aruba Role Enforcement
 - Captive Portal Access: guest-dmz-logon
 - Maximum number of devices allowed per user: 3
 - Guest Access: guest-dmz
3. Everything else can be leave blank or in their default states.



The screenshot shows the 'Access Restrictions' tab selected in a configuration interface. The interface has a top navigation bar with tabs: 'General', 'Wireless Network Settings', 'MAC Caching Settings', 'Posture Settings', and 'Access Restrictions'. Below the tabs, there are three bullet points: 'Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields.', 'Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired.', and 'At least one of Employee, Guest, and Contractor Access must be provided.' Below the bullet points, there is a form with the following fields:

- Enforcement Type*: Aruba Role Enforcement (dropdown menu)
- Captive Portal Access*: guest-dmz-logon (text input)
- Days allowed for access*: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday (checkboxes, all checked)
- Maximum number of devices allowed per user*: 3 (text input)
- Maximum bandwidth allowed per user*: 0 MB (For unlimited bandwidth, set value to 0) (text input)
- Employee Access: (text input)
- Guest Access: guest-dmz-logon (text input)
- Contractor Access: (text input)

At the bottom of the interface, there are buttons: 'Back to Start Here', 'Delete', 'Next >', 'Add Service', and 'Cancel'. The 'Add Service' button is highlighted with a red box.

Figure 113 Access Restrictions Tab

Wizard Summary and Edit Services

ClearPass will notify that you have added a number of profiles, policies, and services that make up this solution. Notice also that *guest-dmz MAC Authentication* and *guest-dmz User Authentication with MAC Caching* were added to the list of services. It is important that MAC Authentication is above User Authentication with MAC Caching. This order enables users to proceed to the self-registration captive portal page only if they fail MAC Authentication.

- **Added 8 Enforcement Profile(s)**
- **Added 2 Enforcement Policies**
- **Added 2 Role Mapping Policies**
- **Added 2 service(s)**

#	<input type="checkbox"/>	Order ▲	Name	Type	Template	Status
1.	<input type="checkbox"/>	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	<input type="checkbox"/>	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
3.	<input type="checkbox"/>	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	●
4.	<input type="checkbox"/>	4	[Guest Operator Logins]	Application	Aruba Application Authentication	●
5.	<input type="checkbox"/>	5	[Insight Operator Logins]	Application	Aruba Application Authentication	●
6.	<input type="checkbox"/>	6	guest-dmz MAC Authentication	RADIUS	MAC Authentication	●
7.	<input type="checkbox"/>	7	guest-dmz User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	●

Figure 114 Wizard Summary and Edit Services